Computers, Materials & Continua
DOI: 10.32604/cmc.2022.031417
Article

Tech Science Press

Generalization of Advanced Encryption Standard Based on Field of Any Characteristic

Nabilah Abughazalah[1], Majid Khan[2,*], Noor Munir[2], Ammar S. Alanazi[3] and Iqtadar Hussain[4,5]

[1]Department of Mathematical Sciences, College of Science, Princess Nourah Bint Abdulrahman University, P.O.Box 84428, Riyadh 11671, Saudi Arabia
[2]Department of Applied Mathematics & Statistics, Institute of Space Technology, Islamabad, Pakistan
[3]King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia
[4]Mathematics Program, Department of Mathematics, Statistics and Physics, College of Arts and Sciences, Qatar University, 2713, Doha, Qatar
[5]Statistical Consulting Unit, College of Arts and Science, Qatar University, Doha, Qatar
*Corresponding Author: Majid Khan. Email: mk.cfd1@gmail.com
Received: 17 April 2022; Accepted: 15 June 2022

Abstract: Nowadays most communications are done by utilizing digital transmission mechanisms. The security of this digital information transmitted through different communication systems is quite important. The secrecy of digital data is one of the burning topics of the digitally developed world. There exist many traditional algorithms in the literature to provide methods for robust communication. The most important and recent modern block cipher named the advanced encryption standard (AES) is one of the extensively utilized encryption schemes with binary based. AES is a succession of four fundamental steps: round key, sub-byte, shift row, and mix column. In this work, we will provide an innovative methodology for extending the AES in a Galois field with any characteristic p. All four steps in the fundamental process with binary characteristics will be adjusted because of the new enhancement. By applying double affine transformations, we have enhanced the number of options in our suggested substitution boxes. The reconstruction of the nonlinear confusion component and encryption structure provides robustness in the generalized AES. The increase in the keyspace due to the Galois field generalization implies that we have improved additional confusion abilities and broadened the current notions. The implementation of the proposed structure of AES for image, audio, and video encryption will provide high security for secure communication.

Keywords: AES; generalized AES; binary field; ternary function

1 Introduction

It is critical to keep secret multimedia material out of the hands of unauthorized parties. Content, music, still images, liveliness, and video are all examples of the interactive media material. Multimedia

security is used to protect these compounds. This is done using cryptographic techniques. These plans foster communication security, robbery, and refugee protection. Encryption is made more difficult by image size [1]. Typically, a typical photograph is of a large scale. Encryption of large amounts of mixed media data will be difficult if a standard encryption technique is used [2]. Due to the large amount of data that must be encrypted, we need to use techniques that demand a minimal amount of computation [3]. Privacy of data is also concerned with the authentication of the source [4,5]. Authentication is provided by some hashing and signature schemes [6,7]. Many encryption structures are protected by digital signature schemes [8]. Numerous studies show the importance of digital signature implementation [9–11]. Digital signatures work on the structure of the asymmetric encryption phenomenon [12]. In comparison to asymmetric key algorithms, private key methods are computationally less genuine. Asymmetric key algorithms are often thousands of times quicker than public-key algorithms [13]. Symmetric key encryption methods provide a more acceptable approach to scrambling interactive media content [14]. It is because of this that the AES symmetric key encryption approach is so fast [15]. In the literature, several novel AES enhancements have been presented [16–19]. In the symmetric block cipher family, the AES is one of the most important, with a key of 128 bits. Typically, the total round in AES is determined by one of three sizes of the secret key utilized in several variations: 128 bits, 192 bits, and 256 bits (10, 12 & 14). A new extension of current AES structures on any characteristic Galois field is our major goal here. Brute-force assaults on encrypted data have been bolstered by the removal of the field of generic prime features [20]. We have added two examples for ternary and quinary finite fields [21,22].

There are four sections in this research article. The basic notions are discussed in segment 2. The suggested scheme along with examples is now discussed in Section 3. Lastly, we have concluded the section.

2 Mathematical Concepts

2.1 Galois Field

A Galois field is a finite field with finite order. The Galois field has an order of prime or an exponent of prime, $GF(p^n)$, as p is prime and represents the field's characteristic and n denotes a positive integer. It is described as:

$$GF(p^n) = \{a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}, a_i \in \mathbb{Z}_p \forall i \in [0, n-1]\}. \tag{1}$$

Now we describe the structure of $GF(3^2)$. Consider $f(x) = x^2 + 2x + 2$ be a primitive irreducible polynomial for $GF(3^2)$. Consider α be the solution of this polynomial thus

$$f(\alpha) = 0, \tag{2}$$

$$\alpha^2 + 2\alpha + 2 = 0, \tag{3}$$

$$\alpha^2 = -2\alpha - 2, \tag{4}$$

As in $GF(3^2)$, $3\alpha + 3 = 0$ therefore we can write it as,

$$\alpha^2 = -2\alpha - 2 + 3\alpha + 3 = \alpha + 1, \alpha^3 = 2\alpha + 1, \alpha^4 = 2, \alpha^5 = 2\alpha, \alpha^6 = 2\alpha + 2, \alpha^7 = \alpha + 2, \alpha^8 = 1. \tag{5}$$

$$GF(3^2) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\} = \{0, 1, \alpha, \alpha + 1, 2\alpha + 1, 2, 2\alpha, 2\alpha + 2, \alpha + 2\}. \tag{6}$$

The elements of $GF(3^2)$ represents the extension field of polynomials with maximum degree one, whose coefficients belongs to $\mathbb{Z}_3$.

2.2 Ternary Logic

There are three sets of assertions or propositions that we will refer to as ternary logic $\{0, 1, 2\}$. To designate this collection, we'll use the set $\mathbb{Z}_3$. It is possible to determine the value of the r proposition by using the map $\mu : \eta \to \mathbb{Z}_3$, as shown below.

$$\mu(r) = \begin{cases} 1 & \text{if } r \text{ is true} \\ 0 & \text{if } r \text{ is either true, or false} \\ 2 & \text{if } r \text{ is false} \end{cases} \tag{7}$$

Consider, if $\mu(r) = 1$, then it is true according to the rules of binary logic, and if $\mu(r) = 1$, then it is true according to the rules of ternary logic. The same is true for the false value. Alternatively, analogous factors are created for binary logic, which we avoid μ by having $\mu(r) = r$. Over η, we describe the subsequent fundamental operations:

- Implication $\to$ (if . . . then)
- Negation $\sim$ (not)
- Conjunction $\wedge$ (and)
- Disjunction $\vee$ (or)

The system η satisfies closure law for the above operations, by this assumption, we can suppose that if $r, s \in \eta$ then $r \vee s \in \eta, \sim r \in \eta, r \wedge s \in \eta$, and $r \to s \in \eta$. Additionally, the proposition in ternary logic is not derived from the other three fundamental operations such as we accomplish in binary logic.

The outcomes in Tab. 1 are $\sim r, r \vee s, r \wedge s$ and $r \to s$ differ in their input r and s. The conjunction and implication equivalency operation are also shown in Tab. 1. Another way to think of these fundamental processes is as functions. The unary operator negation is a function described as $h : \mathbb{Z}_3 \to \mathbb{Z}_3$ and a binary operator can be defined as $h : \mathbb{Z}_3^2 \to \mathbb{Z}_3$. Commonly, we can identify a ternary logic function as mappings $h : \mathbb{Z}_3^n \to \mathbb{Z}_3$.

Table 1: Basic operation in ternary logic

r	s	$\sim r$	$r \wedge s$	$r \wedge s$	$r \to s$	$r \to s$
1	1	2	1	1	1	1
1	0	2	0	1	0	0
1	2	2	2	1	2	2
0	1	0	0	1	1	0
0	0	0	0	0	1	1
0	2	0	2	0	0	0
2	1	1	2	1	1	2
2	0	1	2	0	1	0
2	2	1	2	2	1	1

Unary functions are defined as those in which there is only one solution, and this is the case when n is equal to one. There are $3^{3^1} = 27$ possible solutions, each of which has its own unique set of functions $h(r)$. All 27 of these functions are also referred to as modal functions. The binary function $h(r, s)$ has $3^{3^2} = 19683$ possible outcomes when n is 2 (see Tab. 2).

Table 2: All ternary functions with one variable

x	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_9	h_{10}
0	1	1	1	1	1	1	1	1	1	0
1	0	0	0	2	2	2	1	1	1	0
2	2	1	0	2	1	0	2	1	0	2
x	h_{11}	h_{12}	h_{13}	h_{14}	h_{15}	h_{16}	h_{17}	h_{18}	h_{19}	h_{20}
0	0	0	0	0	0	0	0	0	2	2
1	0	0	2	2	2	1	1	1	0	0
2	1	0	2	1	0	2	1	0	2	1
x	h_{21}	h_{22}	h_{23}	h_{24}	h_{25}	h_{26}	h_{27}			
0	2	2	2	2	2	2	2			
1	0	2	2	2	1	1	1			
2	0	2	1	0	2	1	0			

By utilizing this process, we can calculate $3^{3^3} = 7625597484987$ various functions of several functions. Usually, there exist 3^{3^n} several ternary functions $h(r_1, r_2, \ldots, r_n)$ for n variables.

2.3 S-box Used in AES

An affine transformation $S : GF(2)^n \rightarrow GF(2)^n$ known as a substitution box or S-box is defined by the combination of three functions [7].

$$S = G \circ L \circ M, \tag{8}$$

where L is the linear transformation, M is the inverse transformation, and G is the affine transformation, which can be stated mathematically as follows:

$$M(a) = \begin{cases} a^{-1} & a \neq 0, \\ 0 & a = 0, \end{cases} \tag{9}$$

$$L(a) = Ba, \tag{10}$$

$$G(a) = a \oplus_3 b.$$

As a result, S-box structure is described as

$$\begin{aligned} S(a) &= G(L(M(a))) = G(L(a^{-1})) = G(Ba^{-1}) \\ &= Ba^{-1} \oplus b, \end{aligned} \tag{11}$$

This is the required structure for the S-Box design created on $GF(p)^n$.

2.4 Proposed S-box

S-box is the main non-linear component of the block cipher, which increase the confusion in the algorithm, therefore it must be strong and highly resistant to cryptanalytic attacks. Here we define a new approach to constructing a strong Substitution box. We define a map $S : GF(p)^n \rightarrow GF(p)^n$ by

$$S(x) = A_2.I(A_1x \oplus b_1) \oplus b_2, \tag{12}$$

where A_1, A_2 are linear invertible matrices, b_1, b_2 are column matrices, I is the inverse transformation, and $\oplus$ is rit-wise addition operation under mod p.

2.5 Advanced Encryption Standard

In the context of symmetric algorithms, AES is referred to as a "block cipher." Commercial systems, such as Microsoft's Windows, use it regularly (IPsec, the internet Skype, the IEEE 802.11i, and TLS). AES is referred to as AES-128, AES-192, or AES-256 depending on the size of the key employed in the encryption of the information being protected. Depending on the size of the key, the data matrix has 10, 12, or 14 rounds. $m(x) = x^8 + x^4 + x^3 + x + 1$ is an irreducible polynomial in a finite Galois field of degree 8. The finite Galois field of degree 8 is utilized in the construction of S-box, Sub-byte transformation, and mix column transformation.

3 Generalization of AES on Ternary Logic Function and Double Affine Transformation

Other than binary qualities, we've mostly made use of the extension field in this section. To begin, we must expand the block cipher's nonlinear S-box component to include features 3 and 5, as well as shift row, mix column, and round key. Here we define AES on the plaintext and key of 8-rits with two rounds of encryption, but in general, we can use the desired length of key and plaintext. The round of encryption can also be increased. The working strides of the proposed generalized AES are shown in Fig. 1.

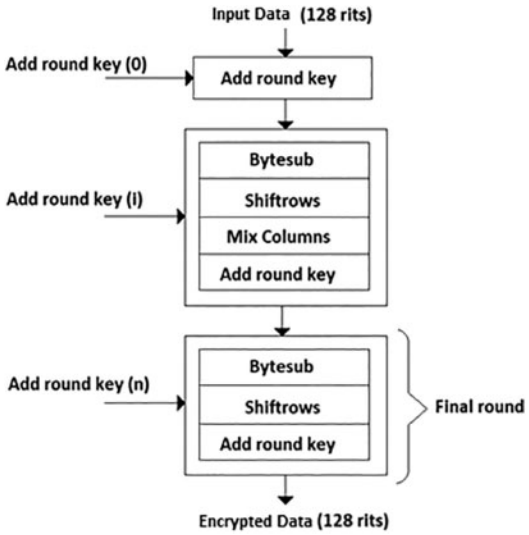

Figure 1: Working strides of proposed generalized AES

3.1 Structure of S-box Created on $GF(3^2)$ and Double Affine Transformation Proposed S-box

A substitution box can be constructed by using the map $S : GF(3)^2 \rightarrow GF(3)^2$ therefore we can write it as

$$S(x) = A_2.I(A_1x \oplus_3 b_1) \oplus_3 b_2, \tag{13}$$

where I represents the inverse transformation and the symbol $\oplus_3$ is rit-wise addition under modulo 3. Now consider the matrices for this expression be

$$A_1 = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, b_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$
$$A_2 = \begin{bmatrix} 0 & 1 \\ 2 & 1 \end{bmatrix}, b_2 = \begin{bmatrix} 0 \\ 2 \end{bmatrix}.$$

The S-box changes to the following value when input values are inserted into the expression (see Tab. 3):

Table 3: S-box on $GF(3^2)$

	0	1	2
0	22	20	00
1	21	02	10
2	01	11	12

The inverse S-box, as shown in the Tab. 4, can be obtained by applying the inverse transformation.

Table 4: Inverse S-box on $GF(3^2)$

	0	1	2
0	02	20	11
1	12	21	22
2	01	10	00

3.2 Proposed AES on $GF(3^2)$

Suppose the plaintext of 8-rits be

$P = 01211020.$

Now we divide this 8-rits plaintext into 4 parts, each consisting of 2-rits

$P_0 = 01, P_1 = 21, P_2 = 10, P_3 = 20.$

The following matrix can be used to represent the simple text:

$$P = \begin{bmatrix} 01 & 10 \\ 21 & 20 \end{bmatrix}.$$

Assume the key be of equal length as plaintext i.e., 8-rits

$K_0 = 10112022.$

The following is a matrix representation of the key:

$$K_0 = \begin{bmatrix} 10 & 20 \\ 11 & 22 \end{bmatrix}.$$

First, we add a key matrix in the plaintext matrix

$$A_1 = P + K_0,$$

$$A_1 = \begin{bmatrix} 01 & 10 \\ 21 & 20 \end{bmatrix} \oplus_3 \begin{bmatrix} 10 & 20 \\ 11 & 22 \end{bmatrix},$$

$$A_1 = \begin{bmatrix} 11 & 00 \\ 02 & 12 \end{bmatrix}.$$

Round 1

Sub-byte Transformation

The first step is to do the sub-byte conversion to each element of the matrix A_1 and we get

$$B_1 = \begin{bmatrix} 02 & 22 \\ 00 & 10 \end{bmatrix}.$$

Shift Row

After shifting the components in the matrix B_1 using the shift row, we get

$$C_1 = \begin{bmatrix} 00 & 11 \\ 21 & 20 \end{bmatrix}.$$

Mix Column

Consider a matrix for the mix column's operation.

$$X = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}.$$

By successively multiplying the X matrix by the C_1 matrix's columns, we arrive to

$$\begin{bmatrix} d_0 \\ d_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 02 \\ 10 \end{bmatrix} = \begin{bmatrix} 12 \\ 20 \end{bmatrix},$$

$$\begin{bmatrix} d_0 \\ d_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 22 \\ 00 \end{bmatrix} = \begin{bmatrix} 22 \\ 00 \end{bmatrix}.$$

In the end, when we combine these two columns into a single matrix, we obtain

$$D_1 = \begin{bmatrix} 12 & 22 \\ 20 & 00 \end{bmatrix}.$$

Key Generation

By using the recent key K_0 we can construct a new key K_1 by using the following procedure

$w_0 = k_0$,
$w_1 = k_1$,
$w_2 = k_2$,
$w_3 = k_3$.
$w_4 = w_0 \oplus_3 Nibble\,sub.(w_3) \oplus_3 rcon(1)$,
$w_5 = w_1 \oplus_3 w_4$,
$w_6 = w_2 \oplus_3 w_5$,
$w_7 = w_2 \oplus_3 w_6$,
$w_4 = 10 \oplus_3 Nibble\,sub.(22) \oplus_3 01 = 20$,
$w_5 = 11 \oplus_3 20 = 01$,
$w_6 = 20 \oplus_3 01 = 21$,
$w_7 = 22 \oplus_3 21 = 10$.

Therefore, the key becomes

$$K_1 = \begin{bmatrix} 20 & 21 \\ 01 & 10 \end{bmatrix}.$$

Key Addition

By adding the key K_1 in the matrix D_1, we get

$$E_1 = D_1 \oplus_3 K_1,$$
$$= \begin{bmatrix} 12 & 22 \\ 20 & 00 \end{bmatrix} \oplus_3 \begin{bmatrix} 20 & 21 \\ 01 & 10 \end{bmatrix},$$
$$E_2 = \begin{bmatrix} 21 & 02 \\ 20 & 00 \end{bmatrix}.$$

Round 2

Sub-byte transformation

We obtain the following as the matrix E_1 has been sub-byte transformed:

$$B_2 = \begin{bmatrix} 00 & 21 \\ 11 & 21 \end{bmatrix}.$$

Shift Row

Shift row is applied to the matrix B_2

$$C_2 = \begin{bmatrix} 00 & 21 \\ 21 & 11 \end{bmatrix}.$$

Mix Column

There is no mix column in the last round

Key Generation

The following procedure can be used to produce the key:

$w_8 = w_0 \oplus_3 Nibble\,sub.(w_7) \oplus_3 rcon(1)$,
$w_9 = w_5 \oplus_3 w_8$,
$w_{10} = w_6 \oplus_3 w_9$,
$w_{11} = w_7 \oplus_3 w_{10}$.
$w_8 = 20 \oplus_3 Nibble\,sub.(10) \oplus_3 10 = 10$,
$w_9 = 01 \oplus_3 21 = 22$,
$w_{10} = 21 \oplus_3 22 = 10$,
$w_{11} = 10 \oplus_3 10 = 20$.

Therefore, the key becomes

$$K_2 = \begin{bmatrix} 21 & 10 \\ 22 & 20 \end{bmatrix}.$$

Key Addition

$$E_2 = C_2 \oplus_3 K_2,$$
$$= \begin{bmatrix} 00 & 21 \\ 21 & 11 \end{bmatrix} \oplus_3 \begin{bmatrix} 21 & 10 \\ 01 & 20 \end{bmatrix},$$
$$E_2 = \begin{bmatrix} 21 & 01 \\ 10 & 01 \end{bmatrix}.$$

The encrypted message is $E_2 = 21100101$.

Decryption

The encrypted data can be decrypted by utilizing the reverse process of encryption.

Round 1

Key subtraction

For decryption, the key matrix K_2 is subtracted from the encrypted matrix E_2 and each element is subtracted from other rit-wise under mod3.

$$C_2 = E_2 - K_2 = \begin{bmatrix} 21 & 01 \\ 10 & 01 \end{bmatrix} - \begin{bmatrix} 21 & 10 \\ 22 & 20 \end{bmatrix},$$
$$C_2 = \begin{bmatrix} 00 & 21 \\ 21 & 11 \end{bmatrix}.$$

Inverse Shift Row

After key subtraction inverse shift row is applied to the matrix C_2

$$B_2 = \begin{bmatrix} 00 & 21 \\ 11 & 21 \end{bmatrix}.$$

Inverse Sub-byte Transformation

After applying inverse shift row, inverse sub-byte transformation is applied by using inverse S-box

$$E_1 = \begin{bmatrix} 02 & 10 \\ 21 & 10 \end{bmatrix}.$$

Round 2

Key Subtraction

Now we subtract the key of round 2 i.e., K_1

$$D_1 = E_1 - K_1 = \begin{bmatrix} 02 & 10 \\ 21 & 10 \end{bmatrix} - \begin{bmatrix} 20 & 21 \\ 01 & 10 \end{bmatrix},$$

$$D_1 = \begin{bmatrix} 12 & 22 \\ 20 & 00 \end{bmatrix}.$$

Inverse Mix Column

In the inverse mix column, we take the inverse of the matrix

$$X = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix},\ X^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}.$$

After multiplying the columns of the matrix D_1 with the matrix X^{-1} one by one we get

$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 12 \\ 20 \end{bmatrix} = \begin{bmatrix} 02 \\ 10 \end{bmatrix},$$

$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 22 \\ 00 \end{bmatrix} = \begin{bmatrix} 22 \\ 00 \end{bmatrix}.$$

After putting these columns together in a matrix,

$$C_1 = \begin{bmatrix} 02 & 22 \\ 10 & 00 \end{bmatrix}.$$

Inverse Shift Row

After utilizing the inverse shift row on the matrix, which is obtained after the inverse mix column, C_1

$$B_1 = \begin{bmatrix} 02 & 22 \\ 00 & 10 \end{bmatrix}.$$

Inverse Sub-byte Transformation

After utilizing inverse Sub-byte transformation by using inverse S-box, we get

$$A_1 = \begin{bmatrix} 11 & 00 \\ 02 & 12 \end{bmatrix}.$$

Key Subtraction

Finally, we subtract the initial key from the matrix A_1, and we get

$$P = A_1 - K_0,$$

$$= \begin{bmatrix} 11 & 00 \\ 02 & 12 \end{bmatrix} - \begin{bmatrix} 10 & 20 \\ 11 & 22 \end{bmatrix},$$

$$P = \begin{bmatrix} 01 & 10 \\ 21 & 20 \end{bmatrix}.$$

Finally, the recovered message is $P = 01211020$.

3.3 Construction of S-box $GF(5^2)$ Based on Double Affine Transformation

A substitution box can be constructed by using the map $S : GF(5)^2 \rightarrow GF(5)^2$ therefore we can write it as

$$S(x) = A_2.I(A_1x \oplus_5 b_1) \oplus_5 b_2,$$

where I represents the inverse transformation and the symbol $\oplus_5$ is rit-wise addition under mod5. Now consider the matrices for this expression be

$$A_2 = \begin{bmatrix} 2 & 4 \\ 0 & 1 \end{bmatrix}, b_2 = \begin{bmatrix} 1 \\ 2 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix}, b_2 = \begin{bmatrix} 0 \\ 4 \end{bmatrix}.$$

As a result, we acquire output values by adding input values into the above formula, the required S-box is given in Tab. 5.

Table 5: S-box on $GF(5^2)$

	0	1	2	3	4
0	00	12	32	11	34
1	13	40	31	04	22
2	41	03	24	42	21
3	10	14	20	23	01
4	44	43	02	30	33

The inverse S-box is shown below in Tab. 6.

Table 6: Inverse S-box on $GF(5^2)$

	0	1	2	3	4
0	00	34	42	21	13
1	30	03	01	10	31

(Continued)

Table 6: Continued

	0	1	2	3	4
2	32	24	14	33	22
3	43	12	02	44	04
4	11	20	23	41	40

3.4 AES Based on $GF(5^2)$

Consider the plaintext of 8-rits be

$P = 01423143.$

Now we divide this 8-rits plaintext into 4 parts, each consisting of 2-rits

$P_0 = 01, P_1 = 42, P_2 = 31, P_3 = 43.$

The following is a matrix representation of the plain text

$$P = \begin{bmatrix} 01 & 31 \\ 42 & 43 \end{bmatrix}.$$

Assume the key be of equal length as plaintext i.e., 8-rits

$K_0 = 40231330.$

Using the matrix form, the key may be expressed as follows:

$$K_0 = \begin{bmatrix} 40 & 13 \\ 23 & 30 \end{bmatrix}.$$

First, we add a key matrix in the plaintext matrix

$A_1 = P \oplus_5 K_0,$

$$A_1 = \begin{bmatrix} 01 & 31 \\ 42 & 43 \end{bmatrix} \oplus_5 \begin{bmatrix} 40 & 13 \\ 23 & 30 \end{bmatrix},$$

$$A_1 = \begin{bmatrix} 41 & 44 \\ 10 & 23 \end{bmatrix}.$$

Round 1

Sub-byte Transformation

Initially, we utilize the S-box transformation to all components of the matrix A_1 and we obtain

$$B_1 = \begin{bmatrix} 43 & 33 \\ 13 & 42 \end{bmatrix}.$$

Shift Row

After employing the shift row to the components of the matrix B_1 we obtain

$$C_1 = \begin{bmatrix} 43 & 33 \\ 42 & 13 \end{bmatrix}.$$

Mix Column

Consider a matrix for the mix column's operation.

$$X = \begin{bmatrix} 1 & 4 \\ 0 & 2 \end{bmatrix}.$$

This is the result of multiplying each column of the matrix C_1 with X one by one

$$\begin{bmatrix} d_0 \\ d_1 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 43 \\ 42 \end{bmatrix} = \begin{bmatrix} 01 \\ 34 \end{bmatrix},$$
$$\begin{bmatrix} d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 33 \\ 13 \end{bmatrix} = \begin{bmatrix} 20 \\ 21 \end{bmatrix}.$$

Combining these two columns into one matrix yields the following result:

$$D_1 = \begin{bmatrix} 01 & 20 \\ 34 & 21 \end{bmatrix}.$$

Key Generation

By using the recent key K_0 we can construct a new key K_1 by using the following procedure

$w_0 = k_0,$
$w_1 = k_1,$
$w_2 = k_2,$
$w_3 = k_3.$
$w_4 = w_0 \oplus_5 Nibble\,sub.(w_3) \oplus_5 rcon(1),$
$w_5 = w_1 \oplus_5 w_4,$
$w_6 = w_2 \oplus_5 w_5,$
$w_7 = w_2 \oplus_5 w_6,$
$w_4 = 10 \oplus_5 Nibble\,sub.(22) \oplus_5 01 = 20,$
$w_5 = 11 \oplus_5 20 = 01,$
$w_6 = 20 \oplus_5 01 = 21,$
$w_7 = 22 \oplus_5 21 = 10.$

Therefore, the key becomes

$$K_1 = \begin{bmatrix} 21 & 32 \\ 24 & 12 \end{bmatrix}.$$

Key Addition

By adding the key K_1 in the matrix D_1, we get

$$E_1 = D_1 \oplus_5 K_1,$$
$$= \begin{bmatrix} 01 & 20 \\ 34 & 21 \end{bmatrix} \oplus_5 \begin{bmatrix} 01 & 32 \\ 24 & 12 \end{bmatrix},$$
$$E_2 = \begin{bmatrix} 02 & 02 \\ 03 & 33 \end{bmatrix}.$$

Round 2

Sub-byte transformation

We obtain the following as the matrix E_1 has been sub-byte transformed:

$$B_2 = \begin{bmatrix} 32 & 32 \\ 11 & 23 \end{bmatrix}.$$

Shift Row

By implementing shift row on the matrix B_2

$$C_2 = \begin{bmatrix} 32 & 32 \\ 23 & 11 \end{bmatrix}.$$

Mix Column

In the last round, there is no mix column.

Key Generation

Keys can be produced in the following way:

$$w_8 = w_0 \oplus_5 Nibble\,sub.(w_7) \oplus_5 rcon(1),$$
$$w_9 = w_5 \oplus_5 w_8,$$
$$w_{10} = w_6 \oplus_5 w_9,$$
$$w_{11} = w_7 \oplus_5 w_{10}.$$
$$w_8 = 01 \oplus_5 Nibble\,sub.(12) \oplus_5 10 = 12,$$
$$w_9 = 24 \oplus_5 12 = 31,$$
$$w_{10} = 32 \oplus_5 31 = 13,$$
$$w_{11} = 12 \oplus_5 13 = 20.$$

Therefore, the key becomes

$$K_2 = \begin{bmatrix} 12 & 13 \\ 31 & 20 \end{bmatrix}.$$

Key Addition

$$E_2 = C_2 \oplus_5 K_2,$$
$$= \begin{bmatrix} 32 & 32 \\ 23 & 11 \end{bmatrix} \oplus_5 \begin{bmatrix} 12 & 13 \\ 31 & 20 \end{bmatrix},$$
$$E_2 = \begin{bmatrix} 44 & 40 \\ 04 & 31 \end{bmatrix}.$$

The encrypted message is $E_2 = 21100101$.

Decryption

The encrypted text can be decrypted by utilizing the reverse process of encryption.

Round 1

Key Subtraction

For decryption, the key matrix K_2 is subtracted from the encrypted matrix E_2 and each element is subtracted from other rit-wise under mod5.

$$C_2 = E_2 - K_2 = \begin{bmatrix} 44 & 40 \\ 04 & 31 \end{bmatrix} - \begin{bmatrix} 12 & 13 \\ 31 & 20 \end{bmatrix},$$

$$C_2 = \begin{bmatrix} 32 & 32 \\ 23 & 11 \end{bmatrix}.$$

Inverse Shift Row

After key subtraction inverse shift row is applied to the matrix C_2

$$B_2 = \begin{bmatrix} 32 & 32 \\ 11 & 23 \end{bmatrix}.$$

Inverse Sub-byte Transformation

After applying inverse shift row, inverse sub-byte transformation is applied by using inverse S-box

$$E_1 = \begin{bmatrix} 02 & 02 \\ 03 & 33 \end{bmatrix}.$$

Round 2

Key subtraction

Now we subtract the key of round 2 i.e., K_1

$$D_1 = E_1 - K_1 = \begin{bmatrix} 02 & 02 \\ 03 & 33 \end{bmatrix} - \begin{bmatrix} 01 & 32 \\ 24 & 12 \end{bmatrix},$$

$$D_1 = \begin{bmatrix} 01 & 20 \\ 34 & 21 \end{bmatrix}.$$

Inverse Mix Column

In the inverse mix column, we take the inverse of the matrix

$$X = \begin{bmatrix} 1 & 4 \\ 0 & 2 \end{bmatrix}, \; X^{-1} = \begin{bmatrix} 1 & 3 \\ 0 & 3 \end{bmatrix}.$$

After multiplying the columns of the matrix D_1 with the matrix X^{-1} one by one we get

$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 01 \\ 34 \end{bmatrix} = \begin{bmatrix} 43 \\ 42 \end{bmatrix},$$

$$\begin{bmatrix} c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 20 \\ 21 \end{bmatrix} = \begin{bmatrix} 33 \\ 13 \end{bmatrix}.$$

After combining these columns in one matrix

$$C_1 = \begin{bmatrix} 43 & 33 \\ 42 & 13 \end{bmatrix}.$$

Inverse Shift Row

After utilizing the inverse shift row on the matrix, which is obtained after the inverse mix column, C_1

$$B_1 = \begin{bmatrix} 43 & 33 \\ 13 & 42 \end{bmatrix}.$$

Inverse Sub-byte Transformation

After employing inverse Sub-byte transformation by using inverse S-box, we get

$$A_1 = \begin{bmatrix} 41 & 44 \\ 10 & 23 \end{bmatrix}.$$

Key Subtraction

Finally, we subtract the initial key from the matrix A_1 , and we get

$$P = A_1 - K_0,$$
$$= \begin{bmatrix} 41 & 44 \\ 10 & 23 \end{bmatrix} - \begin{bmatrix} 40 & 13 \\ 11 & 30 \end{bmatrix},$$
$$P = \begin{bmatrix} 01 & 31 \\ 42 & 43 \end{bmatrix}.$$

Finally, the recovered message is $P = 01423143$.

4 Conclusion

In this paper, we have defined a generalization of AES which gives better results to increase the security of the algorithm. This modifies AES as a complex mathematical structure which is utilizing the composition of two affine nonlinear functions instead of one affine Boolean function as in the case of standard AES. Moreover, the use of different characteristics other than the binary is one of the thought-provoking problems of cryptography. As a result, brute force attacks fail on the modified AES due to increasing the number of possibilities to find the key. The use of ternary and quinary characteristic finite field is yet not used in the development of AES structure. We have utilized ternary and quinary characteristic fields to design a new mathematical foundation for modified AES. The implementation of the generalized AES on hardware is one of the challenging problems for future interests. The designed structure can be utilized for audio and video encryption as well.

Acknowledgement: This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2022R87), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding Statement: This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2022R87), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. M. Shtewi, "An efficient modified advanced encryption standard (MAES) adapted for image cryptosystems," *International Journal of Computer Science and Network Security*, vol. 10, pp. 226–2232, 2010.
[2] S. Lian, "Quasi-commutative watermarking and encryption for secure media content distribution," *Multimedia Tools and Applications*, vol. 43, pp. 91–107, 2009.
[3] K. Gu, W. J. Jia and J. M. Zhang, "Identity-based multi-proxy signature scheme in the standard model," *Fundamenta Informaticae*, vol. 150, no. 2, pp. 179–210, 2017.
[4] K. Gu, W. J. Jia, G. J. Wang and S. Wen, "Efficient and secure attribute-based signature for monotone predicates," *Acta Informatica*, vol. 54, no. 5, pp. 521–541, 2017.
[5] K. Gu, K. M. Wang and L. L. Yang, "Traceable attribute-based signature," *Journal of Information Security and Applications*, vol. 49, pp. 102400, 2019.
[6] K. Gu, W. J. Jia and C. L. Jiang, "Efficient identity-based proxy signature in the standard model," *the Computer Journal*, vol. 58, no. 4, pp. 792–807, 2015.
[7] K. Gu, L. H. Yang, Y. Wang and S. Wen, "Traceable identity-based group signature," *RAIRO-Theoretical Informatics and Applications*, vol. 50, no. 3, pp. 193–226, 2016.
[8] K. Gu, Y. Wang and S. Wen, "Traceable threshold proxy signature," *Journal of Information Science & Engineering*, vol. 33, no. 1, pp. 63–79, 2017.
[9] Z. Xu, C. Xu, J. Xu and X. Meng, "A computationally efficient authentication and key agreement scheme for multi-server switching in WBAN," *International Journal of Sensor Networks*, vol. 35, no. 3, pp. 143–160, 2021.
[10] L. Y. Xiang, X. B. Shen, J. H. Qin and W. Hao, "Discrete multi-graph hashing for large-scale visual search," *Neural Processing Letters*, vol. 49, no. 3, pp. 1055–1069, 2019.
[11] M. A. R. Khan and M. K. Jain, "Feature point detection for repacked android apps," *Intelligent Automation & Soft Computing*, vol. 26, no. 6, pp. 1359–1373, 2020.
[12] N. B. A. Ghani Binti, M. Ahmad, Z. Mahmoud and R. M. Mehmood, "A pursuit of sustainable privacy protection in big data environment by an optimized clustered-purpose based algorithm," *Intelligent Automation & Soft Computing*, vol. 26, no. 6, pp. 1217–1231, 2020.
[13] S. Heron, "Advanced encryption standard (AES)," *Network Security*, vol. 2009, no. 12, pp. 8–12, 2009.
[14] F. B. Muhaya, "Modified AES using chaotic key generator for satellite imagery encryption," *Emerging Intelligent Computing Technology and Applications*, vol. 5754, pp. 1014–1024, 2009.
[15] G. N. Krishnamurthy and V. Ramaswamy, "Making AES stronger: AES with key dependent S-box," *International Journal of Computer Science and Network Security*, vol. 8, pp. 388–398, 2008.
[16] P. Kawle, A. Hiwase, G. Bagde, E. Tekam and R. Kalbande, "Modified advanced encryption standard," *International Journal of Soft Computing and Engineering*, vol. 4, pp. 21–23, 2014.
[17] M. Khan, T. Shah and S. I. Batool, "A new approach for image encryption and watermarking based on substitution box over the classes of chain rings," *Multimedia Tools and Applications*, vol. 76, pp. 24027–24062, 2017.
[18] M. Khan and T. Shah, "Construction and applications of chaotic S-boxes in image encryption," *Neural Comput & Applic*, vol. 27, pp. 677–685, 2016.
[19] M. Khan, T. Shah and S. I. Batool, "A new implementations of chaotic S-boxes in CAPTCHA," *Signal, Image and Video Processing*, vol. 10, pp. 293–300, 2016.

[20] A. Belazi, M. Khan, A. A. Abd El-Latif and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation substitution-based encryption," *Nonlinear Dynamics*, vol. 87, pp. 337–361, 2017.
[21] K. N. Vijeyakumar, V. Sumathy, M. G. Devi, S. Tamilselvan and R. R. Nair, "Design of hardware efficient high speed multiplier using modified ternary logic," *Procedia Engineering*, vol. 38, pp. 2186–219, 2012.
[22] M. Mukaidono, "Regular ternary logic functions; ternary logic functions suitable for treating ambiguity," *IEEE Transactions on Computers*, vol. 35, pp. 179–183, 1986.