A Differential and Linear Analysis of the Inversion Mapping in Odd-Characteristic Finite Fields

Jorge Nakahara Jr

São Paulo, Brazil

Abstract. Substitution boxes (S-boxes) based on the inversion mapping ($S[x] = x^{-1}$) in even-characteristic finite fields are widely used components in the design of cryptographic primitives such as block ciphers (notably the AES cipher). This report focuses on the inversion mapping in finite fields $\mathrm{GF}(p^n)$ where p is a (small) odd prime and n is a (small) integer. We compare the differential and linear profiles of S-boxes over odd- and even-characteristic fields, which also motivates the design and analysis of AES variants operating in fields of odd characteristic. Even for $\mathrm{GF}(2^n)$, the study of S-boxes which are APN permutations (odd-valued n) already shows resistance to differential and linear cryptanalysis after three rounds.

Keywords: odd-characteristic finite fields, inversion mapping, S-box, differential and linear profiles, APN permutations.

1 Introduction

The multiplicative inverse (or simply the inversion) mapping is a widely used component in the design of substitution boxes (S-boxes) which by itseld is a pervasive component in cryptographic primitives such as block ciphers [2, 5, 17, 20], stream ciphers [4] and hash functions [8].

The majority of the cryptographic research so far has focused on inversion mappings in even-characteristic finite fields [14].

Nonetheless, odd-characteristic finite fields are present both in public-key cryptosystems such as Elliptic Curve Cryptography (ECC) [11] and in secret-key cryptosystems [8, 15].

One fact that motivated our research is that the well-known paper [16] studied the inversion mapping in $\mathrm{GF}(2^n)$ for arbitrary n, but not in odd-characteristic finite fields. Other studies that motivated our research include [19, 9].

In this report we study **the differential and linear profiles** of S-boxes based on the pure inversion mappings $S[x] = x^{-1}$ (with the exception that $S[0] = 0$) in odd-characteristic finite fields $\mathrm{GF}(p^n)$, where p is a small prime and n is a small integer.

It is well known that block ciphers such as the AES S-box have an affine transformation layer applied after the inversion mapping to counter interpolation and algebraic attacks and to eliminate fixed points. Since the differential and linear profiles of AES are invariant [3] whether there is an affine transformation or not, we focus attention on the pure inversion mapping. The issue of an appropriate affine transformation is left open for further research.

This paper is organized as follows: Sect.2 provides background on concepts that will be discussed in the paper. Sect.3 describes our experiments with S-boxes based on inversion in GF(3^n) for small values of n. Sect. 4 lists our findings with S-boxes based on inversion in GF(5^n) for small integers n. Sect. 5 describes our results with S-boxes based on inversion in GF(7^n); Sect. 6 presents applications of the results in Sect. 3 to AES variants over GF(3^n); Sect. 7 presents applications of the results in Sect. 4 to AES variants over GF(5^n); Sect. 8 presents applications of the results in Sect. 5 to AES variants over GF(7^n); Sect. 9 summarizes our conclusions.

We do not explore nor compare the software/hardware performance of the AES variants operating on GF(p^n).

2 Preliminaries

A substitution box (S-box) is a nonlinear mapping typically used to provide the property of confusion [18] in a cryptographic design such as block ciphers, stream ciphers and hash functions.

In this report, we are interested in bijective S-boxes, denoted $S : \mathrm{GF}(p^n) \rightarrow \mathrm{GF}(p^n)$, where p is a small prime number and n is a small integer. More specifically, we focus attention on the inversion mapping $S[a] = a^{-1} = a^{p^n-2}$.

For instance, in the AES cipher, the finite field is GF(2^8) =GF(2)[x]/($m(x)$) where $m(x) = x^8 + x^4 + x^3 + x + 1$ and $S[a] = a^{-1} = a^{254}$ for all $a \in \mathrm{GF}(2^8)$.

In a differential cryptanalysis (DC) [1] setting, text blocks are analysed in pairs (t, t^*) and the notion of difference Δ between them usually depends on the operator $\star$ used to mix (sub)keys into the cipher state. In our context, the difference operator is related to the operator in a finite field GF(p^n). For instance, in GF(2^n) the difference operator between two n-bit strings[1] is bitwise exclusive-or, denoted $\Delta = t \oplus t^*$. But, in GF(3^n) the difference operator between two n-trit strings is componentwise subtraction modulo 3.

Concerning differntial cryptanalysis (DC), relevant properties of an S-box include its differential profile and its differential uniformity.

The differential profile is related to the distribution of differences (under an appropriate difference operator $\star$) across its domain.

$$\delta_S(a, b) = \#\{x \in \mathrm{GF}(p^n) : S[x \star a] \star S[x] = b\} \qquad (1)$$

where $a, b \in$GF(p^n). The value a is the input difference, and $b = S[x \star a] \star S[x]$ is the output difference of the S-box S. The usual terminology is to denote that the

[1] A trit is a ternary digit, the GF(3) equivalent of a bit in GF(2)).

(input) difference a leads to the (output) difference b across S with probability $\delta_S(a,b)/p^n$.

The value

$$\delta_{\max} = \max_{a\neq 0, b\neq 0}\delta_S(a,b)$$

is the differential uniformity of S and identifies the most probable nontrivial[2] input/output difference pair(s) (a,b) that can propagate across S.

An extensive listing of $\delta_S(a,b)$ values across all $0 \leq a,b < p^n$ and for a given difference operator $\star$ is called the Difference Distribution Table (DDT) of S.

An S-box S is called differentially $\delta_{\max}$-uniform concerning the difference operator $\star$, that is, all nontrivial entries in its DDT are less than or equal to $\delta_{\max}$. Consequently, the value $\delta_{\max}/p^n$ is the probability of the most probable nontrivial difference propagating across a given S-box S.

Concerning linear cryptanalysis (LC) [13, 12], relevant properties for an S-box include its linear profile and its linear uniformity.

The linear profile concerns the distribution of values that satisfy a given linear relation. Let $< a, x >$ denote the dot product of two strings $a, x \in \mathrm{GF}(p^n)$. So, $< a, x >=< x, a >= \sum_{i=0}^{n-1} a_i \cdot x_i$, where $a = (a_{n-1}, \ldots, a_1, a_0)$, $x = (x_{n-1}, \ldots, x_1, x_0)$ and the sum and product are in $\mathrm{GF}(p^n)$.

Let

$$\gamma_S(a,b) = \#\{x \in \mathrm{GF}(p^n) :< x, a >=< S[x], b >\} - p^{n-1}, \qquad (2)$$

where $a, b \in \mathrm{GF}(p^n)$.

If $\gamma_S(a,b) \neq 0$, there is a nontrivial correlation between a linear combination of input elemets given by the mask a and a linear combination of output elements of S given by the mask b.

The value $\gamma_{\max} = \max_{a\neq 0, b\neq 0}\|\gamma_S(a,b)\|$ indicates the most biased nontrivial linear relation(s) across the S-box S, where $\|i\|$ is the absolute value of i. Notice that $\gamma_S(a,b)$ can be negative. Since we are interested in the magnitude of the bias, we take the absolute value,

The value $\gamma_{\max}$ denotes the linear uniformity of S, and represents the linear counterpart to the differential uniformity.

An extensive listing of $\gamma_S(a,b)$ values for all possible $0 \leq a, b < p^n$ is called the Linear Approximation Table (LAT) of S. The S-box S is therefore linearly $\gamma_{\max}$-uniform, that is, all entries in its LAT are less than or equal to $\gamma_{\max}$.

Consequently, the value $\gamma_{\max}/p^n$ represents the bias of the most probable nontrivial linear relation propagating across a given S-box S.

3 Inversion in GF(3^n)

The first S-boxes using the inversion mapping in odd-characteristic finite fields for which we experimentally computed the differential and linear profiles were over GF(3^n) for small integers n.

[2] The trivial difference is the case $a = b = 0$.

In GF(3), each individual element $x \in \{0, 1, 2\}$ is called a **trit** which stands for a single ternary digit.

We adopted polynomial bases [10] for representing GF(3^n) for different values of n. Table 1 lists the irreducible polynomials we used in our experiments. These polynomials were obtained from the GP/PARI calculator version 2.9.4.

Table 1. Constructing GF(3^n) =GF(3)[x]/($m(x)$) for small values of n using polynomial bases. n is the number of trits.

n	irreducible polynomials $m(x)$	Field size
2	$x^2 + 2x + 2$	9
3	$x^3 + 2x + 1$	27
4	$x^4 + 2x^3 + x^2 + x + 2$	81
5	$x^5 + 2x^3 + 2x^2 + x + 1$	243
6	$x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2$	729
7	$x^7 + 2x^6 + 2x^5 + x^4 + x^3 + 2x + 1$	2187
8	$x^8 + x^7 + x^6 + 2x^5 + 2x^4 + x^2 + 2$	6561

We could have tested GF(3^n) for $n > 8$ but the storage cost of these S-boxes increases exponentially. The third column of Table 1 shows the field size which is also the size of each S-box.

Constructing S-boxes in GF(3^n) (or more generally, in GF(p^n)) from the ground up can be done using several different techniques. For instance, using Fermat's Little Theorem [14], $x^{-1} = x^{p^n-2}$, and the S-box can be constructed by repeated square and multiply operations modulo $m(x)$ for each n. An efficient approach to compute inversion is to decompose the exponent $p^n - 2$ using the Itoh-Tsujii algorithm [7]. This algorithm may be an alternative if the S-box is too large to store.

Alternatively, exponentiation (g^t) and logarithmic ($\log_g t$) tables can be computed from a generator g of GF(3^n) and nonzero $t \in$ GF$(3^n)^*$ [3]. These tables allow straightforward computation of the multiplication and division of any two nonzero elements $a, b \in$ GF$(p^n)^*$. There might be $z, y \in$ GF$(p^n)^*$ such that $a = g^z$ and $b = g^y$. So, $z = \log_g a$ and $y = \log_g b$. Consequently, $a \cdot b = g^z \cdot g^y = g^{z+y} = g^{\log_g a + \log_g b}$. Likewise, $a/b = g^z/g^y = g^{z-y} = g^{\log_g a - \log_g b}$. The inversion operation is a special case of division: $a^{-1} = 1/a = 1/g^z = g^{-z} = g^{p^n-1-\log_g a}$.

Table 2. An S-box based on inversion in GF(3^2) = GF(3)[x]/($x^2 + 2x + 2$).

i	0	1	2	3	4	5	6	7	8
$S[i]$	0	1	2	5	8	3	7	6	4

The difference operator for polynomials GF(3^n) is componentwise subtraction modulo 3.

The first example of an S-box in GF(3^n) is for $n = 2$ and is depicted in Table 2.

The DDT of the S-box in Table 2 is depicted in Table 3.

Table 3. DDT of S-box in Table 2. Input difference (ID) in rows. Output difference (OD) in columns. All values in decimal base.

	OD								
ID	0	1	2	3	4	5	6	7	8
0	9	0	0	0	0	0	0	0	0
1	0	3	2	2	0	0	0	2	0
2	0	2	3	0	0	2	2	0	0
3	0	2	0	0	2	3	0	2	0
4	0	0	0	2	2	2	0	0	3
5	0	0	2	3	2	0	2	0	0
6	0	0	2	0	0	2	0	3	2
7	0	2	0	2	0	0	3	0	2
8	0	0	0	0	3	0	2	2	2

The LAT of the S-box in Table 2 is depicted in Table 4.

Table 4. LAT of S-box in Table 2. Input mask (IM) in rows. Output mask (OM) in columns. All values in decimal base.

	OM								
IM	0	1	2	3	4	5	6	7	8
0	6	0	0	0	0	0	0	0	0
1	0	0	0	-2	4	-2	2	2	2
2	0	0	0	2	2	2	-2	-2	4
3	0	-2	2	4	2	0	2	0	-2
4	0	4	2	2	0	-2	-2	2	0
5	0	-2	2	0	-2	2	0	4	2
6	0	2	-2	2	-2	0	4	0	2
7	0	2	-2	0	2	4	0	2	-2
8	0	2	4	-2	0	2	2	-2	0

The differential and linear uniformities of the S-boxes based on inversion in GF(3^n) are listed in Table 5.

Comparatively, for the AES S-box, we can scale its dimension down and obtain the results in Table 6. Notice that for even n, the inversion mapping in GF(2^n) is differentially 4-uniform, while for odd n this mapping is differentially

Table 5. Differential and linear uniformity of S-boxes based on the inversion mapping in GF(3^n) for small values of n.

n	δmax (prob.)	$\|\gamma$max$\|$ (bias)
2	3 ($3/3^2 = 3^{-1} \approx 2^{-1.584}$)	4 ($4/3^2 \approx 2^{-1.169}$)
3	3 ($3/3^3 = 3^{-2} \approx 2^{-3.169}$)	6 ($6/3^3 \approx 2^{-2.169}$)
4	3 ($3/3^4 = 3^{-3} \approx 2^{-4.754}$)	12 ($12/3^4 \approx 2^{-2.754}$)
5	3 ($3/3^5 = 3^{-4} \approx 2^{-6.339}$)	20 ($20/3^5 \approx 2^{-3.602}$)
6	3 ($3/3^6 = 3^{-5} \approx 2^{-7.924}$)	36 ($36/3^6 \approx 2^{-4.339}$)
7	3 ($3/3^7 = 3^{-6} \approx 2^{-9.509}$)	62 ($62/3^7 \approx 2^{-5.140}$)
8	3 ($3/3^8 = 3^{-7} \approx 2^{-11.094}$)	108 ($108/3^8 \approx 2^{-5.924}$)

2-uniform that is, for odd n the inversion mappings in GF(2^n) are Almost Perfect Nonlinear (APN) mappings [16].

Table 6. Differential and linear uniformity of S-boxes based on the inversion mapping in GF(2^n) for small values of n.

n	δmax (prob.)	$\|\gamma$max$\|$ (bias)
3	2 ($2/2^3 = 2^{-2}$)	2 ($2/2^3 = 2^{-2}$)
4	4 ($4/2^4 = 2^{-2}$)	4 ($4/2^4 = 2^{-2}$)
5	2 ($2/2^5 = 2^{-4}$)	6 ($6/2^5 \approx 2^{-2.41}$)
6	4 ($4/2^6 = 2^{-4}$)	8 ($8/2^6 = 2^{-3}$)
7	2 ($2/2^7 = 2^{-6}$)	10 ($10/2^7 \approx 2^{-3.67}$)
8	4 ($4/2^8 = 2^{-6}$)	16 ($16/2^8 = 2^{-4}$)

An interesting aspect in Table 5 is that the differential uniformity of all the S-boxes in GF(3^n) is 3, which stands in between the uniformity of the S-boxes based on inversion in GF(2^n) (2 and 4 depending on n). The differential uniformities for S-boxes in GF(3^n) are partially corroborated by [8] for $n = 3$.

Comparatively, the linear uniformities of the S-boxes in GF(3^n) are strictly less than the corresponding uniformities for the S-boxes in GF(2^n) for $3 \leq n \leq 8$.

4 Inversion in GF(5^n)

In GF(5), each individual element $x \in \{0, 1, 2, 3, 4\}$ is called a **pit** which stands for a single penta-ary digit.

We adopt polynomial bases [10] for representing GF(5^n) for different values of n. Table 7 lists the irreducible polynomial we used for our experiments. These polynomials were obtained from the GP/PARI calculator version 2.9.4.

The third column of Table 7 shows the field size which is also the size (number of entries) of each S-box.

Table 7. Constructing GF(5^n) = GF(5)$[x]/(m(x))$ for small values of n using polynomial bases.

n	irreducible polynomials $m(x)$	Field size
2	x^2+x+2	25
3	x^3+3x^2+x+2	125
4	x^4+4x^3+2x+2	625
5	$x^5+2x^3+x^2+2x+2$	3125
6	x^6+x^2+2x+2	15625

The difference operator $\star$ used for polynomials in GF(5^n) is (componentwise) subtraction modulo 5.

The first example of an S-box in GF(5^n) is for $n = 2$ and is depicted in Table 8. Entries are in decimal.

Table 8. An S-box based on inversion in GF(5^2) = GF(5)$[x]/(x^2+x+2)$.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
$S[i]$	0	1	3	2	4	12	10	9	19	7	6	22	5	16	17	24	13	14	20	8	18	23	11	21	15

The DDT of the S-box in Table 8 is depicted in Table 9.

The LAT of the S-box in Table 8 is depicted in Table 10.

The differential and linear uniformity of S-boxes based on inversion in GF(5^n) are listed in Table 11.

The alternation of 2 and 4 in $\delta_{\max}$ in GF(5^n) for odd and even n respectively in Table 11 is exactly the same as observed for inversion in GF(2^n) in Table 6. The S-boxes in GF(5^n) are APN for odd n, just like for GF(2^n).

5 Inversion in GF(7^n)

In GF(7), each individual element $x \in \{0,1,2,3,4,5,6\}$ is called a **hit** which stands for a single hepta-ary digit.

We adopt polynomial bases [10] for representing GF(7^n) for different values of n. Table 12 lists the irreducible polynomial we used for our experiments. These polynomials were obtained from the GP/PARI calculator version 2.9.4.

The third column of Table 12 shows the field size which is also the size of each S-box.

The difference operator $\star$ used for polynomials in GF(7^n) is (componentwise) subtraction modulo 7.

The differential and linear uniformities of the S-boxes based on inversion in GF(7^n) are listed in Table 13.

Table 9. DDT of S-box in Table 8. Input difference (ID) in rows. Output difference (OD) in columns.

	OD																								
ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	4	2	2	1	2	0	0	0	0	2	2	0	2	0	0	2	0	2	2	0	0	0	0	2
2	0	2	1	4	2	2	0	0	2	2	0	0	2	0	0	2	0	0	0	0	0	0	2	2	2
3	0	2	4	1	2	0	2	2	2	0	2	0	0	0	0	0	0	0	2	0	2	2	2	0	0
4	0	1	2	2	4	0	2	0	0	0	0	2	2	0	2	2	0	2	0	2	2	0	0	0	0
5	0	2	2	0	0	0	2	0	2	2	2	0	4	0	2	0	2	2	1	0	0	0	0	0	2
6	0	0	0	2	2	2	0	2	2	0	4	0	2	2	0	1	2	2	0	0	2	0	0	0	0
7	0	0	0	2	0	0	2	0	2	4	2	2	0	2	0	2	0	2	2	0	0	1	0	2	0
8	0	0	2	2	0	2	2	2	2	2	0	1	0	2	2	0	0	0	0	4	0	0	2	0	0
9	0	0	2	0	0	2	0	4	2	0	0	2	2	0	2	2	2	0	2	0	0	2	0	1	0
10	0	2	0	2	0	2	4	2	0	0	0	0	2	0	0	0	0	2	2	2	0	2	0	2	1
11	0	2	0	0	2	0	0	2	1	2	0	2	0	0	0	2	2	2	2	2	0	0	4	0	0
12	0	0	2	0	2	4	2	0	0	2	2	0	0	0	0	2	2	0	0	2	1	2	0	2	0
13	0	2	0	0	0	0	2	2	2	0	0	0	0	2	1	2	4	0	0	2	2	0	0	2	2
14	0	0	0	0	2	2	0	0	2	2	0	0	0	1	2	0	0	4	2	2	2	2	0	0	2
15	0	0	2	0	2	0	1	2	0	2	0	2	2	2	0	0	0	0	2	0	2	0	0	2	4
16	0	2	0	0	0	2	2	0	0	2	0	2	2	4	0	0	2	1	0	0	2	2	2	0	0
17	0	0	0	0	2	2	2	2	0	0	2	2	0	0	4	0	1	2	0	0	0	0	2	2	2
18	0	2	0	2	0	1	0	2	0	2	2	2	0	0	2	2	0	0	0	0	4	2	0	0	2
19	0	2	0	0	2	0	0	0	4	0	2	2	2	2	2	0	0	0	0	2	0	2	1	2	0
20	0	0	0	2	2	0	2	0	0	0	0	0	1	2	2	2	2	0	4	0	0	2	2	0	2
21	0	0	0	2	0	0	0	1	0	2	2	0	2	0	2	0	2	0	2	2	2	0	2	4	0
22	0	0	2	2	0	0	0	0	2	0	0	4	0	0	0	0	2	2	0	1	2	2	2	2	2
23	0	0	2	0	0	0	0	2	0	1	2	0	2	2	0	2	0	2	0	2	0	4	2	0	2
24	0	2	2	0	0	2	0	0	0	0	1	0	0	2	2	4	0	2	2	0	2	0	2	2	0

6 AES variants over GF(3^n)

In this section we will describe our experiments in replacing the AES S-box with each of the S-boxes described in Sect. 3 therefore creating AES variants operating on GF(3^n).

6.1 AES variants operating on GF(3^n) and a 3×3 state

Let us consider AES variants with:

- word size of n trits
- 3×3 square states that is, the block size is $9n$ trits
- internal operations on GF(3^n) for different values of n
- the key size is at least $9n$ trits
- the same high-level round structure as the AES [3] consisting of SubBytes, ShiftRows, MixColumns and AddRoundKey in this order, but:

Table 10. LAT of S-box in Table 8. Input mask (IM) in rows. Output mask (OM) in columns.

	OM																								
IM	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	-2	2	2	-2	0	0	-4	-2	6	0	2	0	4	4	0	4	4	0	2	0	6	-2	-4	0
2	0	2	-2	-2	2	0	0	4	2	4	0	-2	0	6	-4	0	-4	6	0	-2	0	4	2	4	0
3	0	2	-2	-2	2	0	0	4	2	4	0	-2	0	6	-4	0	-4	6	0	-2	0	4	2	4	0
4	0	-2	2	2	-2	0	0	-4	-2	6	0	2	0	4	4	0	4	4	0	2	0	6	-2	-4	0
5	0	0	0	0	0	4	-2	2	-4	0	6	4	2	0	-2	6	-2	0	2	4	4	0	-4	2	-2
6	0	0	0	0	0	-2	2	6	0	4	2	0	-2	-4	4	2	4	-4	-2	0	-2	4	0	6	2
7	0	-4	4	4	-4	2	6	2	0	0	-2	0	4	0	-2	-2	-2	0	4	0	2	0	0	2	6
8	0	-2	2	2	-2	-4	0	0	6	-2	4	4	0	2	0	4	0	2	0	4	-4	-2	6	0	0
9	0	6	4	4	6	0	4	0	-2	-2	0	2	-4	2	0	0	0	2	-4	2	0	-2	-2	0	4
10	0	0	0	0	0	6	2	-2	4	0	4	-4	-2	0	2	4	2	0	-2	-4	6	0	4	-2	2
11	0	2	-2	-2	2	4	0	0	4	2	-4	6	0	-2	0	-4	0	-2	0	6	4	2	4	0	0
12	0	0	0	0	0	2	-2	4	0	-4	-2	0	2	4	6	-2	6	4	2	0	2	-4	0	4	-2
13	0	4	6	6	4	0	-4	0	2	2	0	-2	4	-2	0	0	0	-2	4	-2	0	2	2	0	-4
14	0	4	-4	-4	4	-2	4	-2	0	0	2	0	6	0	2	2	2	0	6	0	-2	0	0	-2	4
15	0	0	0	0	0	6	2	-2	4	0	4	-4	-2	0	2	4	2	0	-2	-4	6	0	4	-2	2
16	0	4	-4	-4	4	-2	4	-2	0	0	2	0	6	0	2	2	2	0	6	0	-2	0	0	-2	4
17	0	4	6	6	4	0	-4	0	2	2	0	-2	4	-2	0	0	0	-2	4	-2	0	2	2	0	-4
18	0	0	0	0	0	2	-2	4	0	-4	-2	0	2	4	6	-2	6	4	2	0	2	-4	0	4	-2
19	0	2	-2	-2	2	4	0	0	4	2	-4	6	0	-2	0	-4	0	-2	0	6	4	2	4	0	0
20	0	0	0	0	0	4	-2	2	-4	0	6	4	2	0	-2	6	-2	0	2	4	4	0	-4	2	-2
21	0	6	4	4	6	0	4	0	-2	-2	0	2	-4	2	0	0	0	2	-4	2	0	-2	-2	0	4
22	0	-2	2	2	-2	-4	0	0	6	-2	4	4	0	2	0	4	0	2	0	4	-4	-2	6	0	0
23	0	-4	4	4	-4	2	6	2	0	0	-2	0	4	0	-2	-2	-2	0	4	0	2	0	0	2	6
24	0	0	0	0	0	-2	2	6	0	4	2	0	-2	-4	4	2	4	-4	-2	0	-2	4	0	6	2

- SubBytes uses an S-box in GF(3^n) from Table 1
- ShiftRows operates on a 3×3 state of n-trit words, and the left-shift amounts are by 0, 1 and 2 words from the top to the bottom row
- MixColumns uses a 3×3 MDS matrix with components over GF(3^n). We do not provide these matrices explicitly for each n, but we assume they exist.
- AddRoundKey uses addition in GF(3^n) instead of exclusive-or

With these assumptions, we expect to achieve full text diffusion after every two rounds just like in AES.

The exact details of the key schedule algorithm for the AES variants are not relevant for our analyses.

The choice of a 3×3 state for a text block and a 3×3 MDS matrix instead of a 4×4 state and a 4×4 MDS matrix (as in the AES) was arbitrary but it seems a natural generalization in view of the new finite field GF(3^n).

Table 11. Differential and linear uniformity of S-boxes based on the inversion mapping in GF(5^n) for small values of n.

n	δmax (prob.)	$\|\gamma$max$\|$ (bias)
2	4 ($4/5^2 \approx 2^{-2.643}$)	6 ($6/5^2 \approx 2^{-2.058}$)
3	2 ($2/5^3 \approx 2^{-5.965}$)	14 ($14/5^3 \approx 2^{-3.158}$)
4	4 ($4/5^4 \approx 2^{-7.287}$)	36 ($36/5^4 \approx 2^{-4.117}$)
5	2 ($2/5^5 \approx 2^{-10.609}$)	80 ($80/5^5 \approx 2^{-5.287}$)
6	4 ($4/5^6 \approx 2^{-11.931}$)	198 ($198/5^6 \approx 2^{-6.302}$)

Table 12. Constructing GF(7^n) =GF(7)[x]/($m(x)$) for small values of n using polynomial bases.

n	irreducible polynomials $m(x)$	Field size
2	$x^2 + 5x + 5$	49
3	$x^3 + 4x^2 + 3x + 2$	343
4	$x^4 + x^3 + 3x^2 + 2x + 3$	2401
5	$x^5 + 2x^4 + 4x^3 + 2x^2 + 4x + 2$	16807

With these assumptions and starting from a single non-zero difference word in the plaintext, the number of active S-boxes across four consecutive rounds are at least: 1, 3, 9 and 3, respectively. This is a similar pattern of active S-boxes in AES (which uses a 4×4 state) across four rounds: 1, 4, 16 and 4.

While in AES there are at least 25 active S-boxes after 4 full rounds, in the AES variant there are at least 16 active S-boxes. These assumptions provide an upperbound on the probability of any characteristic covering up to four rounds.

The number of text pairs that can be constructed for a differential attack depends on the number of active words in the input (plaintext). If there is only one active word difference (and 8 passive words) in the input, then the number of pairs is $(3^n * (3^n - 1)/2) \cdot 3^{8n} \approx 3^{10n}/2$ pairs. If the inverse of the probability of the characteristic is larger than the number of available text pairs then the attack is not feasible.

Under these assumptions, we can compare how many rounds of the AES variants are needed for each variant to withstand a conventional differential attack. Results are displayed in Table 14. The number of chosen plaintext pairs

Table 13. Differential and linear uniformity of S-boxes based on the inversion mapping in GF(7^n) for small values of n.

n	δmax (prob.)	$\|\gamma$max$\|$ (bias)
2	4 ($4/7^2 \approx 2^{-3.614}$)	8 ($8/7^2 \approx 2^{-2.614}$)
3	4 ($4/7^3 \approx 2^{-6.422}$)	22 ($22/7^3 \approx 2^{-3.962}$)
4	4 ($4/7^4 \approx 2^{-9.229}$)	72 ($72/7^4 \approx 2^{-5.059}$)
5	4 ($4/7^5 \approx 2^{-12.036}$)	190 ($190/7^5 \approx 2^{-6.466}$)

Table 14. DC resistance of AES variants operating on GF(3^n) and a 3×3 state.

n	Codebook size	#text pairs	Probability (upperbound)		
	(3^{9n})	($3^{10n}/2$)	2 rounds	3 rounds	4 rounds
2	3^{18}	$3^{20}/2$	3^{-4}	3^{-13}	3^{-16}
3	3^{27}	$3^{30}/2$	3^{-8}	$3^{-2\cdot 13} = 3^{-26}$	$3^{-2\cdot 16} = 3^{-32}$
4	3^{36}	$3^{40}/2$	3^{-12}	$3^{-3\cdot 13} = 3^{-39}$	$3^{-3\cdot 16} = 3^{-48}$
5	3^{45}	$3^{50}/2$	3^{-16}	$\mathbf{3}^{-4\cdot 13} = 3^{-52}$	$3^{-4\cdot 16} = 3^{-64}$
6	3^{54}	$3^{60}/2$	3^{-20}	$\mathbf{3}^{-5\cdot 13} = 3^{-65}$	$3^{-5\cdot 16} = 3^{-80}$
7	3^{63}	$3^{70}/2$	3^{-24}	$\mathbf{3}^{-6\cdot 13} = 3^{-78}$	$3^{-6\cdot 16} = 3^{-96}$
8	3^{72}	$3^{80}/2$	3^{-28}	$\mathbf{3}^{-7\cdot 13} = 3^{-91}$	$3^{-7\cdot 16} = 3^{-112}$

for a successfull differential attack is estimated to be proportional to the inverse of the probability of the characteristic whose number of active S-boxes is shown in Table 14.

From Table 14, two rounds are not enough to resist DC for any n. For $n > 4$, three rounds are enough to counter conventional differential attacks. This is a slightly better result than for the original AES cipher which requires at least four rounds.

It is intuitive to look at what happens after three rounds because starting from a single active word, the maximum number of active words is reached after three rounds[3]: 1, 3, 9. The same phenomenon happens in any AES variant operating on square-shaped states be it 3×3 or larger.

For LC in GF(3^n), we consider the estimate in [6] for the number of known plaintexts needed for a linear attack: $N = (\prod_{\#\text{ active S-boxes}} \gamma\text{max}/3^n)^{-2}$.

Similar to the differential case and under the assumptions for the AES variant in GF(3^n), the expected minimum number of active S-boxes across four consecutive rounds is: 1, 3, 9 and 3, respectively.

The results of the linear analyses are summarized in Table 15. From Table 15,

Table 15. LC resistance of AES variants operating on GF(3^n) and a 3×3 state.

n	Codebook	#known plaintexts		
	size (3^{9n})	2 rounds	3 rounds	4 rounds
2	3^{18}	$(4/3^2)^{4*(-2)} \approx 3^{5.905}$	$(4/3^2)^{-2*13} \approx 3^{19.191}$	$(4/3^2)^{-2*16} \approx 3^{23.620}$
3	3^{27}	$(6/3^3)^{4*(-2)} \approx 3^{10.952}$	$(6/3^3)^{-2*13} \approx 3^{35.595}$	$(6/3^3)^{-2*16} \approx 3^{43.810}$
4	3^{36}	$(12/3^4)^{4*(-2)} \approx 3^{13.905}$	$(12/3^4)^{-2*13} \approx 3^{45.191}$	$(12/3^4)^{-2*16} \approx 3^{55.620}$
5	3^{45}	$(20/3^5)^{4*(-2)} \approx 3^{18.185}$	$(20/3^5)^{-2*13} \approx 3^{59.102}$	$(20/3^5)^{-2*16} \approx 3^{72.741}$
6	3^{54}	$(36/3^6)^{4*(-2)} \approx 3^{21.905}$	$(36/3^6)^{-2*13} \approx 3^{71.191}$	$(36/3^6)^{-2*16} \approx 3^{87.620}$
7	3^{63}	$(62/3^7)^{4*(-2)} \approx 3^{25.946}$	$(62/3^7)^{-2*13} \approx 3^{84.326}$	$(62/3^7)^{-2*16} \approx 3^{103.786}$
8	3^{72}	$(108/3^8)^{4*(-2)} \approx 3^{29.905}$	$(108/3^8)^{-2*13} \approx 3^{97.191}$	$(108/3^8)^{-2*16} \approx 3^{119.620}$

[3] This fact is due to the round construction, a combination of ShiftRows and a $n \times n$ MDS matrix.

two rounds are not enough to protect any of the AES variants in GF(3^n) against LC. But, after three rounds, for $n > 2$, the number of known plaintexts needed for a linear attack already exceeds the codebook size. This is a slightly better result than for the original AES cipher which requires four rounds.

6.2 AES variants operating on GF(3^n) and a 4×4 state

Now, for comparison purposes, let us consider the original framework of AES: 4×4 state and 4×4 MDS matrix.

In this setting, full text diffusion is still reached after every two rounds, and the number of active S-boxes across four consecutive rounds follows the pattern: 1, 4, 16 and 4 respectively. So, after 2, 3 and 4 rounds the cummulative number of active S-boxes (for DC and LC) is 5, 21 and 25, respectively. Based on these assumptions, Table 16 shows the resistance to DC. Table 17 shows the resistance to LC.

Table 16. DC resistance of AES variants operating on GF(3^n) and a 4×4 state.

n	Codebook size	#text pairs	Probability (upperbound)		
	(3^{16n})	($3^{17n}/2$)	2 rounds	3 rounds	4 rounds
2	3^{32}	$3^{34}/2$	3^{-5}	$3^{-1*21} = 3^{-21}$	3^{-25}
3	3^{48}	$3^{51}/2$	3^{-10}	$3^{-2*21} = 3^{-42}$	$3^{-2*25} = 3^{-50}$
4	3^{64}	$3^{68}/2$	3^{-15}	$3^{-3*21} = 3^{-36}$	$3^{-3*25} = 3^{-75}$
5	3^{80}	$3^{85}/2$	3^{-20}	$3^{-4*21} = 3^{-84}$	$3^{-4*25} = 3^{-100}$
6	3^{96}	$3^{102}/2$	3^{-30}	$3^{-5*21} = 3^{-105}$	$3^{-5*25} = 3^{-125}$
7	3^{112}	$3^{119}/2$	3^{-35}	$3^{-6*21} = 3^{-126}$	$3^{-6*25} = 3^{-150}$
8	3^{128}	$3^{136}/2$	3^{-40}	$3^{-7*21} = 3^{-147}$	$3^{-7*25} = 3^{-175}$

From Table 16, two rounds are not enough to protect this AES variant against conventional DC for any n. But, three rounds are enough for $n \geq 6$. This is a slightly better result than for AES which requires four rounds.

From Table 17, two rounds are not enough to protect this AES variant for any n. For three rounds, protection against LC is achieved for $n > 2$. This is a slightly better result than for AES for which four rounds are needed.

Therefore, the use of 3×3 or 4×4 states does not matter. Using an appropriate word size n, it is possible to achieve resistance against DC and LC with three rounds (compared to four rounds for the original AES cipher). Consequently, the hypothesized AES variants can operate under a smaller number of rounds than the original AES (or likewise, under a larger margin of security).

As a matter of fact, even for the original 4×4 state of AES, the APN S-boxes for $n \in \{7, 9\}$ in Table 6 already provided resistance to DC after three rounds. See Table 18. For $n = 8$, that is for the original AES, three rounds are not enough to protect it against DC.

Table 17. LC resistance of AES variants operating on GF(3^n) and a 4×4 state.

n	Codebook size (3^{16n})	#known plaintexts		
		2 rounds	3 rounds	4 rounds
2	3^{32}	$(4/3^2)^{5*(-2)} \approx 3^{7.38}$	$(4/3^2)^{-2*21} \approx 3^{31.00}$	$(4/3^2)^{-2*25} \approx 3^{36.90}$
3	3^{48}	$(6/3^3)^{5*(-2)} \approx 3^{13.69}$	$(6/3^3)^{-2*21} \approx 3^{57.50}$	$(6/3^3)^{-2*25} \approx 3^{68.45}$
4	3^{64}	$(12/3^4)^{5*(-2)} \approx 3^{17.38}$	$(12/3^4)^{-2*21} \approx 3^{73.00}$	$(12/3^4)^{-2*25} \approx 3^{86.90}$
5	3^{80}	$(20/3^5)^{5*(-2)} \approx 3^{22.73}$	$(20/3^5)^{-2*21} \approx 3^{95.47}$	$(20/3^5)^{-2*25} \approx 3^{113.65}$
6	3^{96}	$(36/3^6)^{5*(-2)} \approx 3^{27.38}$	$(36/3^6)^{-2*21} \approx 3^{115.00}$	$(36/3^6)^{-2*25} \approx 3^{136.90}$
7	3^{112}	$(62/3^7)^{5*(-2)} \approx 3^{32.43}$	$(62/3^7)^{-2*21} \approx 3^{136.21}$	$(62/3^7)^{-2*25} \approx 3^{162.16}$
8	3^{128}	$(108/3^8)^{5*(-2)} \approx 3^{37.38}$	$(108/3^8)^{-2*21} \approx 3^{157.00}$	$(108/3^8)^{-2*25} \approx 3^{186.90}$

Table 18. DC resistance of AES (variants) operating on a 4×4 state over GF(2^n).

n	Codebook size (2^{16n})	#text pairs ($2^{17n}/2$)	Probability (upperbound)		
			2 rounds	3 rounds	4 rounds
3	2^{48}	$2^{51}/2$	$2^{-2*5} = 2^{-10}$	$2^{-2*21} = 2^{-42}$	$2^{-2*25} = 2^{-50}$
5	2^{80}	$2^{85}/2$	$2^{-4*5} = 2^{-20}$	$2^{-4*21} = 2^{-84}$	$2^{-4*25} = 2^{-100}$
7	2^{112}	$2^{119}/2$	$2^{-6*5} = 2^{-30}$	$\mathbf{2}^{-6*21} = 2^{-126}$	$\mathbf{2}^{-6*25} = 2^{-150}$
8	2^{128}	$2^{136}/2$	$2^{-6*5} = 2^{-30}$	$2^{-6*21} = 2^{-126}$	$\mathbf{2}^{-6*25} = 2^{-150}$
9	2^{144}	$2^{153}/2$	$2^{-8*5} = 2^{-40}$	$\mathbf{2}^{-8*21} = 2^{-168}$	$\mathbf{2}^{-8*25} = 2^{-200}$

Concerning LC, all APN S-boxes (for odd n) in Table 6 are resistant to conventional LC after three rounds.

For $n = 8$, that is for the original AES, three rounds are enough to protect it against LC.

The results in Tables 18 and 19 show that a reduction by a single factor of two in the differential and linear uniformities (the case of APN permutations in GF(2^n) for odd n.) already have an impact in decreasing the minimum number of rounds needed to protect these AES variants against DC and LC.

7 AES variants over GF(5^n)

In this section we will describe our experiments in replacing the AES S-box with each of the S-boxes described in Sect. 4 therefore creating AES variants operating on GF(5^n).

7.1 AES variants operating on GF(5^n) and a 5×5 state

Let us consider AES variants with:

- word size of n pits (Sect. 4)
- 5×5 square states that is the block size is $25n$ pits
- internal operations on GF(5^n) for different values of n

Table 19. LC resistance of AES variants operating on a 4×4 state over GF(2^n).

n	Codebook	#known plaintexts		
	size (2^{16n})	2 rounds	3 rounds	4 rounds
3	2^{48}	$(2/2^3)^{-2*5} = 2^{20}$	$(2/2^3)^{-2*21} = 2^{84}$	$(2/2^3)^{-2*25} = 2^{100}$
5	2^{80}	$(6/2^5)^{-2*5} \approx 2^{24.15}$	$(6/2^5)^{-2*21} \approx 2^{101.43}$	$(6/2^5)^{-2*25} \approx 2^{120.75}$
7	2^{112}	$(10/2^7)^{-2*5} \approx 2^{36.78}$	$(10/2^7)^{-2*21} \approx 2^{154.47}$	$(10/2^7)^{-2*25} \approx 2^{183.90}$
8	2^{128}	$(2^{-4})^{-10} = 2^{40}$	$(2^{-4})^{-42} = 2^{168}$	$(2^{-4})^{-50} = 2^{200}$
9	2^{144}	$(22/2^9)^{-10} = 2^{45.4}$	$(22/2^9)^{-42} = 2^{190.68}$	$(22/2^9)^{-50} = 2^{227.00}$

- the key size is at least $25n$ trits
- the same high-level round structure as the AES [3] consisting of SubBytes, ShiftRows, MixColumns and AddRoundKey in this order, but:
  - SubBytes uses an S-box in GF(5^n) from Table 7
  - ShiftRows operates on a 5×5 state of n-pit words, and the left-shift amounts are by 0, 1, 2, 3 and 4 words from the top to the bottom row
  - MixColumns uses a 5×5 MDS matrix with components over GF(5^n). We do not provide these matrices explicitly for each n, but we assume they exist.
  - AddRoundKey uses addition in GF(5^n) instead of exclusive-or

With these assumptions, we expect to achieve full text diffusion after every two rounds just like in AES.

The exact details of the key schedule algorithm for the AES variants are not relevant for our analyses.

The choice of a 5×5 state for a text block and a 5×5 MDS matrix instead of a 4×4 state and a 4×4 MDS matrix (as in the AES) was arbitrary but it seems a natural generalization in view of the larger finite field GF(5^n)

With these assumptions and starting from a single non-zero difference word in the plaintext, the number of active S-boxes across four consecutive rounds are at least: 1, 5, 25 and 5, respectively. This is a similar pattern as the number of active S-boxes in the original AES across four rounds: 1, 4, 16 and 4.

Cummulatively, in AES there are at least 1, 5, 21 and 25 active S-boxes after 1, 2, 3 and 4 full rounds, respectively, both in a DC and a LC setting. In the new AES variants there are at least 1, 6, 31 and 36 active S-boxes, respectively.

The number of text pairs that can be constructed for a differential attack depends on the number of active words in the input (plaintext). If there is only one active word difference (and all other words are passive) in the input, then the number of pairs is $(5^n * (5^n - 1)/2) \cdot 5^{24n} \approx 5^{26n}/2$ pairs. If the inverse of the probability of the characteristic is larger than the number of available text pairs then the attack is not feasible.

Under these assumptions, we can compare how many rounds of the AES variants are needed for each variant to withstand a conventional differential attack. Results are displayed in Table 20. the number of chosen plaintext pairs for a successfull differential attack is estimated to be proportional to the inverse

Table 20. DC resistance of AES variants operating on GF(5^n) and a 5×5 state.

n	#text pairs	Probability (upperbound)		
	($5^{26n}/2$)	2 rounds	3 rounds	4 rounds
2	$5^{52}/2$	$(4/5^2)^6 \approx 5^{-6.831}$	$(4/5^2)^{31} \approx 5^{-35.298}$	$(4/5^2)^{36} \approx 5^{-40.991}$
3	$5^{78}/2$	$(2/5^3)^6 \approx 5^{-15.415}$	$(2/5^3)^{31} \approx 5^{-79.649}$	$(2/5^3)^{36} \approx 5^{-92.495}$
4	$5^{104}/2$	$(4/5^4)^6 \approx 5^{-18.831}$	$(4/5^4)^{31} \approx 5^{-97.298}$	$(4/5^4)^{36} \approx 5^{-112.991}$
5	$5^{130}/2$	$(2/5^5)^6 \approx 5^{-27.415}$	$(2/5^5)^{31} \approx 5^{-141.649}$	$(2/5^5)^{36} \approx 5^{-164.495}$
6	$5^{156}/2$	$(4/5^6)^6 \approx 5^{-30.831}$	$(4/5^6)^{31} \approx 5^{-159.298}$	$(4/5^6)^{36} \approx 5^{-184.991}$

of the probability of the characteristic whose number of active S-boxes is shown in Table 20.

From Table 20, two rounds is not enough to resist DC for any n. For $n \in \{3, 5, 6\}$, three rounds are enough to counter conventional differential attacks. This is a slightly better result than for the original AES cipher which requires at least four rounds.

For LC in GF(5^n), we consider the estimate in [6] for the number of known plaintexts needed for a linear attack: $N = (\prod_{\#\text{ active S-boxes}} \gamma\text{max}/5^n)^{-2}$.

Similar to the differential case and under the assumptions for the AES variant in GF(5^n), the expected minimum number of active S-boxes across four consecutive rounds is: 1, 6, 31 and 36, respectively.

The results of the linear analyses are summarized in Table 21.

Table 21. LC resistance of AES variants operating on GF(5^n) and a 5×5 state.

n	Codebook	#known plaintexts		
	size (5^{25n})	2 rounds	3 rounds	4 rounds
2	5^{50}	$(6/5^2)^{-2*6} \approx 5^{10.640}$	$(6/5^2)^{-2*31} \approx 5^{54.976}$	$(6/5^2)^{-2*36} \approx 5^{63.842}$
3	5^{75}	$(14/5^3)^{-2*6} \approx 5^{16.322}$	$(14/5^3)^{-2*31} \approx 5^{84.336}$	$(14/5^3)^{-2*36} \approx 5^{97.938}$
4	5^{100}	$(36/5^4)^{-2*6} \approx 5^{21.280}$	$(36/5^4)^{-2*31} \approx 5^{109.952}$	$(36/5^4)^{-2*36} \approx 5^{127.686}$
5	5^{125}	$(80/5^5)^{-2*6} \approx 5^{27.326}$	$(80/5^5)^{-2*31} \approx 5^{141.192}$	$(80/5^5)^{-2*36} \approx 5^{163.964}$
6	5^{150}	$(198/5^6)^{-2*6} \approx 5^{32.570}$	$(198/5^6)^{-2*31} \approx 5^{168.280}$	$(198/5^6)^{-2*36} \approx 5^{195.422}$

From Table 21, two rounds are not enough to protect any of the AES variants in GF(5^n) against LC. But, three rounds are enough to counter a conventional differential attack for any n.

7.2 AES variants operating on GF(5^n) and a 4×4 state

Now, for comparison purposes, let us consider the original framework of AES: a 4×4 state and 4×4 MDS matrix. We assume that such MDS matrices over GF(5^n) exist.

In this setting, full text diffusion is still reached after every two rounds, and the number of active S-boxes across four consecutive rounds follows the pattern: 1, 4, 16 and 4, respectively. So, after 2, 3 and 4 rounds the cummulative number of active S-boxes (for DC and LC) is 5, 21 and 25, respectively. Based on these assumptions, Table 22 shows the resistance to DC. Table 23 shows the resistance to LC.

Table 22. DC resistance of AES variants operating on GF(5^n) and a 4×4 state.

n	Codebook size	#text pairs	Probability (upperbound)		
	(5^{16n})	($5^{17n}/2$)	2 rounds	3 rounds	4 rounds
2	5^{32}	$5^{34}/2$	$(4/5^2)^5 \approx 5^{-5.693}$	$(4/5^2)^{21} \approx 5^{-23.911}$	$(4/5^2)^{25} \approx 5^{-28.466}$
3	5^{48}	$5^{51}/2$	$(2/5^3)^5 \approx 5^{-12.846}$	$(2/5^3)^{21} \approx 5^{-53.955}$	$(2/5^3)^{25} \approx 5^{-64.233}$
4	5^{64}	$5^{68}/2$	$(4/5^4)^5 \approx 5^{-15.693}$	$(4/5^4)^{21} \approx 5^{-65.911}$	$(4/5^4)^{25} \approx 5^{-78.466}$
5	5^{80}	$5^{85}/2$	$(2/5^5)^5 \approx 5^{-22.846}$	$(2/5^5)^{21} \approx 5^{-95.955}$	$(2/5^5)^{25} \approx 5^{-114.233}$
6	5^{96}	$5^{102}/2$	$(4/5^6)^5 \approx 5^{-25.693}$	$(4/5^6)^{21} \approx 5^{-107.911}$	$(4/5^6)^{25} \approx 5^{-128.466}$

From Table 22, two rounds are not enough to protect this AES variant against conventional DC for any n. But, three rounds are enough for $n \in \{3, 5, 6\}$. This is a slightly better result than for AES which requires four rounds.

Table 23. LC resistance of AES variants operating on GF(5^n) and a 4×4 state.

n	Codebook	#known plaintexts		
	size (5^{16n})	2 rounds	3 rounds	4 rounds
2	5^{32}	$(6/5^2)^{-2*5} \approx 5^{8.867}$	$(6/5^2)^{-2*21} \approx 5^{37.242}$	$(6/5^2)^{-2*25} \approx 5^{44.33}$
3	5^{48}	$(14/5^3)^{-2*5} \approx 5^{13.602}$	$(14/5^3)^{-2*21} \approx 5^{57.130}$	$(14/5^3)^{-2*25} \approx 5^{68.01}$
4	5^{64}	$(36/5^4)^{-2*5} \approx 5^{17.734}$	$(36/5^4)^{-2*21} \approx 5^{74.484}$	$(36/5^4)^{-2*25} \approx 5^{88.67}$
5	5^{80}	$(80/5^5)^{-2*5} \approx 5^{22.772}$	$(80/5^5)^{-2*21} \approx 5^{95.646}$	$(80/5^5)^{-2*25} \approx 5^{113.86}$
6	5^{96}	$(198/5^6)^{-2*5} \approx 5^{27.142}$	$(198/5^6)^{-2*21} \approx 5^{113.997}$	$(198/5^6)^{-2*25} \approx 5^{135.71}$

From Table 23, two rounds are not enough to protect this AES variant against LC for any n. For three rounds, protection against LC is achieved for all $2 \leq n \leq 6$. This is a slightly better result than for AES for which four rounds are needed.

Therefore, the use of a 5 or a 4×4 state does not matter. Using an appropriate word size n it is possible to achieve resistance against DC and LC with three rounds (compared to four rounds for the original AES cipher over GF(2^8)). Consequently, the new AES variants can potentially operate under a smaller number of rounds than the original AES (or likewise, under a larger margin of security).

8 AES variants over GF(7^n)

In this section we will describe our experiments in replacing the AES S-box with each of the S-boxes described in Sect. 5 therefore creating AES variants operating on GF(7^n).

8.1 AES variants operating on GF(7^n) and a 7×7 state

Let us consider AES variants with:

- word size of n pits (Sect. 5)
- 7×7 square states that is the block size is $49n$ pits
- internal operations on GF(7^n) for different values of n
- the key size is at least $49n$ trits
- the same high-level round structure as the AES [3] consisting of SubBytes, ShiftRows, MixColumns and AddRoundKey in this order, but:
  - SubBytes uses an S-box in GF(7^n) from Table 12
  - ShiftRows operates on a 7×7 state of n-pit words, and the i-th row is left-shifted by i words $0 \leq i \leq 6$, from the top to the bottom row
  - MixColumns uses a 7×7 MDS matrix with components over GF(7^n). We do not provide these matrices explicitly for each n, but we assume they exist.
  - AddRoundKey uses addition in GF(7^n) instead of exclusive-or

With these assumptions, we expect to achieve full text diffusion after every two rounds just like in AES.

The exact details of the key schedule algorithm for the AES variants are not relevant for our analyses.

The choice of a 7×7 state for a text block and a 7×7 MDS matrix instead of a 4×4 state and a 4×4 MDS matrix (as in the AES) was arbitrary but it seems a natural generalization in view of the larger finite field GF(7^n)

With these assumptions and starting from a single non-zero difference word in the plaintext, the number of active S-boxes across four consecutive rounds are at least: 1, 7, 49 and 7, respectively. This is a similar pattern as the number of active S-boxes in the original AES across four rounds: 1, 4, 16 and 4.

Cummulatively, in AES there are at least 1, 5, 21 and 25 active S-boxes after 1, 2, 3 and 4 full rounds, respectively, both in a DC and a LC setting. In the new AES variants there are at least 1, 8, 57 and 64 active S-boxes, respectively.

The number of text pairs that can be constructed for a differential attack depends on the number of active words in the input (plaintext). If there is only one active word difference (and 48 passive words) in the input, then the number of pairs is $(7^n * (7^n - 1)/2) \cdot 7^{48n} \approx 7^{50n}/2$ pairs. If the inverse of the probability of the characteristic is larger than the number of available text pairs then the attack is not feasible.

Under these assumptions, we can compare how many rounds of the AES variants are needed for each variant to withstand a conventional differential

Table 24. DC resistance of AES variants operating on GF(7^n) and a 7×7 state.

n	#text pairs	Probability (upperbound)		
	($7^{50n}/2$)	2 rounds	3 rounds	4 rounds
2	$7^{100}/2$	$(4/7^2)^8 \approx 7^{-10.30}$	$(4/7^2)^{57} \approx 7^{-73.39}$	$(4/7^2)^{64} \approx 7^{-82.40}$
3	$7^{150}/2$	$(4/7^3)^8 \approx 7^{-18.30}$	$(4/7^3)^{57} \approx 7^{-130.39}$	$(4/7^3)^{64} \approx 7^{-146.40}$
4	$7^{200}/2$	$(4/7^4)^8 \approx 7^{-26.30}$	$(4/7^4)^{57} \approx 7^{-187.39}$	$(4/7^4)^{64} \approx 7^{-210.40}$
5	$7^{250}/2$	$(4/7^5)^8 \approx 7^{-34.30}$	$(4/7^5)^{57} \approx 7^{-244.39}$	$(4/7^5)^{64} \approx 7^{-274.40}$

attack. Results are displayed in Table 20. the number of chosen plaintext pairs for a successfull differential attack is estimated to be proportional to the inverse of the probability of the characteristic whose number of active S-boxes is shown in Table 24.

From Table 24, two or three rounds are not enough to resist DC for any n. For $n \in \{4, 5\}$, four rounds is needed to counter conventional differential attacks. This is the same result as for the original AES cipher.

For LC in GF(7^n), we consider the estimate in [6] for the number of known plaintexts needed for a linear attack: $N = (\prod_{\#\text{ active S-boxes}} \gamma\text{max}/7^n)^{-2}$.

Similar to the differential case and under the assumptions for the AES variant in GF(7^n), the expected minimum number of active S-boxes across four consecutive rounds is: 1, 8, 57 and 64, respectively.

The results of the linear analyses are summarized in Table 25.

Table 25. LC resistance of AES variants operating on GF(7^n) and a 7×7 state.

n	Codebook	#known plaintexts		
	size (7^{50n})	2 rounds	3 rounds	4 rounds
2	7^{100}	$(8/7^2)^{-2*8} \approx 7^{14.90}$	$(8/7^2)^{-2*57} \approx 7^{106.17}$	$(8/7^2)^{-2*64} \approx 7^{119.21}$
3	7^{150}	$(22/7^3)^{-2*8} \approx 7^{22.58}$	$(22/7^3)^{-2*57} \approx 7^{160.91}$	$(22/7^3)^{-2*64} \approx 7^{180.67}$
4	7^{200}	$(72/7^4)^{-2*8} \approx 7^{28.83}$	$(72/7^4)^{-2*57} \approx 7^{205.45}$	$(72/7^4)^{-2*64} \approx 7^{230.68}$
5	7^{250}	$(190/7^5)^{-2*8} \approx 7^{36.85}$	$(190/7^5)^{-2*57} \approx 7^{262.60}$	$(190/7^5)^{-2*64} \approx 7^{294.85}$

From Table 25, two rounds are not enough to protect any of the AES variants in GF(7^n) against LC. But, three rounds are enough to counter a conventional differential attack for any n, $2 \leq n \leq 5$.

8.2 AES variants operating on GF(7^n) and a 4×4 state

Now, for comparison purposes, let us consider the original framework of AES: a 4×4 state and 4×4 MDS matrix. We assume that such MDS matrices over GF(7^n) exist.

In this setting, full text diffusion is still reached after every two rounds, and the number of active S-boxes across four consecutive rounds follows the pattern:

1, 4, 16 and 4, respectively. So, after 2, 3 and 4 rounds the cummulative number of active S-boxes (for DC and LC) is 5, 21 and 25, respectively. Based on these assumptions, Table 26 shows the resistance to DC. Table 27 shows the resistance to LC.

Table 26. DC resistance of AES variants operating on GF(7^n) and a 4×4 state.

n	Codebook size	#text pairs	Probability (upperbound)		
	(7^{16n})	($7^{17n}/2$)	2 rounds	3 rounds	4 rounds
2	7^{32}	$7^{34}/2$	$(4/7^2)^5 \approx 7^{-6.43}$	$(4/7^2)^{21} \approx 7^{-27.03}$	$(4/7^2)^{25} \approx 7^{-32.18}$
3	7^{48}	$7^{51}/2$	$(4/7^3)^5 \approx 7^{-11.43}$	$(4/7^3)^{21} \approx 7^{-48.03}$	$(4/7^3)^{25} \approx 7^{-57.18}$
4	7^{64}	$7^{68}/2$	$(4/7^4)^5 \approx 7^{-16.43}$	$(4/7^4)^{21} \approx 7^{-69.03}$	$(4/7^4)^{25} \approx 7^{-82.18}$
5	7^{80}	$7^{85}/2$	$(4/7^5)^5 \approx 7^{-21.43}$	$(4/7^5)^{21} \approx 7^{-90.03}$	$(4/7^5)^{25} \approx 7^{-107.18}$

From Table 26, two rounds are not enough to protect this AES variant against conventional DC for any n. But, three rounds are enough for $n \in \{4, 5\}$. This is a slightly better result than for AES which requires four rounds.

Table 27. LC resistance of AES variants operating on GF(7^n) and a 4×4 state.

n	Codebook	#known plaintexts		
	size (7^{16n})	2 rounds	3 rounds	4 rounds
2	7^{32}	$(8/7^2)^{-2*5} \approx 7^{9.31}$	$(8/7^2)^{-2*21} \approx 7^{39.11}$	$(8/7^2)^{-2*25} \approx 7^{46.56}$
3	7^{48}	$(22/7^3)^{-2*5} \approx 7^{14.11}$	$(22/7^3)^{-2*21} \approx 7^{59.28}$	$(22/7^3)^{-2*25} \approx 7^{70.57}$
4	7^{64}	$(72/7^4)^{-2*5} \approx 7^{18.02}$	$(72/7^4)^{-2*21} \approx 7^{75.69}$	$(72/7^4)^{-2*25} \approx 7^{90.11}$
5	7^{80}	$(190/7^5)^{-2*5} \approx 7^{23.03}$	$(190/7^5)^{-2*21} \approx 7^{96.74}$	$(190/7^5)^{-2*25} \approx 7^{115.17}$

From Table 27, two rounds are not enough to protect this AES variant against LC for any n. For three rounds, protection against LC is achieved for all $2 \leq n \leq 5$. This is a slightly better result than for AES for which four rounds are needed.

9 Conclusions

In this paper, we study the differential and linear profiles of S-boxes based on the inversion mapping in odd-characteristic finite fields GF(p^n) for small prime p and small integer n.

A previous experimental result [8] described a hash function called Troika operating on GF(3^3). Troika used a 3×3-trit S-box, but they did not provide a theoretical justification for the differential and linear profiles of their S-box.

Nonetheless, this setting may indicate a potential application of the S-boxes we studied to cryptocurrencies which operate on ternary fields such as IOTA.

Our results listed in Tables 5, 11 and 13 show differential and linear uniformity (obtained experimentally) of S-boxes in GF(3^n), GF(5^n) and GF(7^n), respectively.

These findings led us to study new AES variants operating in odd-characteristic fields. As an example, new AES variants operating on 3×3 states composed of n-trit words showed resistance to DC and LC after three rounds, according to the results in Tables 14 and 15. This result is slightly better than for the AES which requires four rounds.

Table 18 and 19 show the differential and linear uniformity for S-boxes based on inversion in GF(2^n) for odd-valued n, and the number of rounds needed to resist DC and LC.

A summary of our results concerning DC of AES variants is in Table 28. A summary of our results concerning LC of AES variants is in Table 29.

Table 28. Summary of DC of AES variants operating on GF(p^n), p prime and n integer.

State Size	Finite Field			
	GF(2^n)	GF(3^n)	GF(5^n)	GF(7^n)
3×3	—	3 rounds, $n > 4$	—	
4×4	4 rounds, $n = 8$ 3 rounds, $n \in \{7, 9\}$	3 rounds, $n > 6$	3 rounds, $n \in \{3, 5, 6\}$	3 rounds, $n \in \{4, 5\}$
5×5	—	—	3 rounds, $n \in \{3, 5, 6\}$	—
7×7	—	—	—	4 rounds, $n \in \{4, 5\}$

Table 29. Summary of LC of AES variants operating on GF(p^n), p prime and n integer.

State Size	Finite Field			
	GF(2^n)	GF(3^n)	GF(5^n)	GF(7^n)
3×3	—	3 rounds, $n > 2$	—	
4×4	4 rounds, $n = 8$ 3 rounds, $n \in \{7, 9\}$	3 rounds, $n > 2$	3 rounds, $2 \leq n \leq 6$	3 rounds, $2 \leq n \leq 5$
5×5	—	—	3 rounds, $2 \leq n \leq 6$	—
7×7	—	—	—	3 rounds, $2 \leq n \leq 5$

References

1. E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer, 1993.
2. J. Daemen, L. R. Knudsen, and V. Rijmen. The Block Cipher SQUARE. In E. Biham, editor, *Fast Software Encryption (FSE)*, LNCS 1267, pages 149–165. Springer, 1997.
3. J. Daemen and V. Rijmen. *The Design of Rijndael, AES - The Advanced Encryption Standard*. Springer, 2002.
4. ETSI. Specification of the 3GPP confidentiality and integrity algorithms UEA2 and UIA2. Document 2: SNOW specification, Ver. 1.1, 2006.
5. FIPS197. Advanced Encryption Standard (AES). FIPS PUB 197 Federal Information Processing Standard Publication 197, United States Department of Commerce, 2001.
6. L. Granboulan, E. Levieil, and G. Piret. Pseudorandom permutation families over Abelian groups. In M.J.B. Robshaw, editor, *Fast Software Encryption (FSE)*, LNCS 4047, pages 57–77, 2006.
7. T. Itoh and S. Tsujii. A fast algorithm for computing multiplicative inverses in GF(2^n). *Information and Computation*, 78(3):171–177, 1988.
8. S. Kolbl, E. Tischhauser, P. Derbez, and A. Bogdanov. Troika: a ternary cryptographic hash function. *Designs, Codes and Cryptography*, 88:91–117, 2020.
9. A. Kostyk, V. Hlukhov, and L. Berezko. The research of multiplication in the ternary Galois fields. Internatioanl Youth Science Forum "Litteris Et Artbus, Nov. 2017.
10. R. Lidl and H. Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2008.
11. W. Mahmoud and H. Wu. Accelerating finite field inversion in GF(3^m) for Elliptic Curve Cryptography. *Applied Mathematics and Information Sciences, Natural Sciences Pub*, 10(5):1645–1655, 2016.
12. M. Matsui. Linear Cryptanalysis of DES Cipher (I), ver. 1.03.
13. M. Matsui. Linear Cryptanalysis Method for DES Cipher. In T. Helleseth, editor, *Advances in Cryptology, Eurocrypt*, LNCS 765, pages 386–397. Springer, 1993.
14. A. J. Menezes, P.C. Van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.
15. C. Moraga, M. Stankovic, and R. Stankovic. Generalized permutations and ternary bent functions. Technical report, Technische Universitat Dortmund, 2019.
16. K. Nyberg. Differentially Uniform Mappings for Cryptography. In T. Helleseth, editor, *Advances in Cryptology, Eurocrypt*, LNCS 765, pages 55–64. Springer, 1993.
17. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. De, Win. The Cipher SHARK. In D. Gollmann, editor, *Fast Software Encryption (FSE)*, LNCS 1039, pages 99–112. Springer, 1996.
18. C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715, 1949.
19. Jessie Tank. Ternary Computing. http://reddit/com/r/iota/comments/7z4c4y/jessie-tanks-awesome-technical-talk-on-the, 2016.
20. Toshiba. Specification of Hierocrypt-3. First NESSIE Workshop, Heverlee, Belgium, 2000.