Projective Aspects of the AES Inversion

Wen-Ai Jackson and Sean Murphy

Technical Report
RHUL–MA–2006–4
25 November 2005

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England
http://www.rhul.ac.uk/mathematics/techreports

Projective Aspects of the AES Inversion

Wen-Ai Jackson[1] and S. Murphy[2]

[1]Dept of Mathematics,
University of Adelaide,
Adelaide, S.A. 5005, Australia

[2]Information Security Group,
Royal Holloway, University of London,
Egham, Surrey TW20 0EX, U.K.

Abstract. We consider the nonlinear function used in the Advanced Encryption Standard (AES). This nonlinear function is essentially inversion in the finite field $\mathrm{GF}(2^8)$, which is most naturally considered as a projective transformation. Such a viewpoint allows us to demonstrate certain properties of this AES nonlinear function. In particular, we make some comments about the group generated by such transformations, and we give a characterisation for the values in the AES *Difference* or XOR *Table* for the AES nonlinear function and comment on the geometry given by this XOR Table.

1 Introduction

The Advanced Encryption Standard (AES) [8, 20] uses only one nonlinear function, namely the mapping of the finite field $\mathrm{GF}(2^8)$ to itself defined by $x \mapsto x^{2^8-2}$. However, this AES nonlinear function maps the multiplicative group $\mathrm{GF}(2^8)^*$ to itself and is just finite field inversion for an element of this multiplicative group. Thus the AES nonlinear function is really just finite field inversion, but which has been extended to the whole field $\mathrm{GF}(2^8)$ by requiring that $0 \mapsto 0$. A round of the AES consists of the simultaneous application of this nonlinear function to each byte of the state space, followed by a linear diffusion function of the entire state space and finally a subkey addition.

It is clear that the properties of this nonlinear function are critical to the security of the AES. However, it is also clear that an "inversion" mapping such as that of the AES is probably most naturally handled mathematically in terms of projective geometry, and in particular in terms of the projective line of the finite field. Indeed, some such geometric aspects of the AES inversion mapping, such as the cross-ratio, have already been discussed in [1]. In this paper, we consider such a projective approach to analysing the AES nonlinear function and discuss some consequences of this adopting this point of view. We begin by giving a very brief general discussion of the relevant aspects of projective geometry. We then consider some consequences of this approach for the group-theoretic properties of AES-like transformations and for the differential properties of the AES inversion function.

2 Projective Geometry

We consider the binary finite field $\mathbb{F} = \mathrm{GF}(2^n)$, where the case for $n = 8$ is of special interest to us because of the AES. We denote the multiplicative group of the field $\mathbb{F}$ by $\mathbb{F}^*$, so $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$. We let $f: \mathbb{F} \mapsto \mathbb{F}$ denote the AES nonlinear function, so $f(x) = x^{2^n-2}$. As the AES nonlinear function is inversion on $\mathbb{F}^*$, we also use the notation $x^{(-1)}$ to denote $f(x)$. We now discuss the projective line of $\mathbb{F}$ and then more general projective geometries over $\mathbb{F}$. A much more thorough discussion is given in [11].

We define the projective line $\overline{\mathbb{F}}$ of $\mathbb{F}$ by considering the two-dimensional vector space $\mathbb{F}^2$ over $\mathbb{F}$. The *projective line* $\overline{\mathbb{F}}$ of $\mathbb{F}$ is the set of all one-dimensional subspaces of this two-dimensional vector space $\mathbb{F}^2$, and any such one-dimensional is a *point* on the projective line $\overline{\mathbb{F}}$. Loosely speaking, the projective line $\overline{\mathbb{F}}$ is the set of all lines through the origin in the plane defined by $\mathbb{F}$. Thus the projective line $\overline{\mathbb{F}}$ of $\mathbb{F}$ consists of all lines or projective points $\langle(1, z)\rangle$ for $z \in \mathbb{F}$ together with the "point at infinity" $\langle(0, 1)\rangle$. We let the line or projective point $\langle(1, z)\rangle$ correspond to the point $z \in \overline{\mathbb{F}}$ in this usual projective manner, and the point at infinity $\langle(0, 1)\rangle$ correspond to the symbol $\infty \in \overline{\mathbb{F}}$. In other words, the projective line $\overline{\mathbb{F}}$ of $\mathbb{F}$ is the finite field $\mathbb{F}$ together with a point at infinity. In summary, we have $\overline{\mathbb{F}} = \mathbb{F} \cup \{\infty\} = \mathbb{F}^* \cup \{0, \infty\}$.

The projective transformations of the projective line $\overline{\mathbb{F}}$ are given by the invertible linear transformations of the two-dimensional vector space $\mathbb{F}^2$ ([11] Chapter 6). If T is an invertible linear transformation of $\mathbb{F}^2$, then T maps any one-dimensional subspace of $\mathbb{F}^2$ to some other one-dimensional subspace and so gives a mapping of the points of $\overline{\mathbb{F}}$. The group of all such transformations is the *projective general linear* group acting on $\overline{\mathbb{F}}$, and is denoted for the projective line by $\mathrm{PGL}(2, \mathbb{F})$. With the usual conventions about ∞, $\mathrm{PGL}(2, \mathbb{F})$ is the set of all fractional linear transformations of $\overline{\mathbb{F}}$ ([22] Theorem 9.46), so

$$\mathrm{PGL}(2, \mathbb{F}) = \left\{ \overline{g}: \overline{\mathbb{F}} \to \overline{\mathbb{F}} \;\middle|\; \overline{g}(x) = \frac{ax + b}{cx + d}, \quad ad + bc \neq 0 \right\}.$$

For even characteristic, it is well-known that there is an isomorphism between $\mathrm{PGL}(2, \mathbb{F})$ and the *special linear* group $\mathrm{SL}(2, \mathbb{F})$ of unimodular (determinant 1) 2×2 matrices ([11] Theorem 2.8). This isomorphism is given by $\eta: \mathrm{PGL}(2, \mathbb{F}) \to \mathrm{SL}(2, \mathbb{F})$, which is defined by

$$\eta\left(x \mapsto \frac{ax + b}{cx + d}\right) = \frac{1}{ad + bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Furthermore, the group actions of $\mathrm{PGL}(2, \mathbb{F})$ on $\overline{\mathbb{F}}$ and $\mathrm{SL}(2, \mathbb{F})$ acting on the lines of the 2-dimensional vector space over $\mathbb{F}$ are isomorphic. Thus we may identify a 2×2 matrix with determinant 1 with a fractional linear transformation, that is a projective transformation of the projective line $\overline{\mathbb{F}}$, and vice versa.

The AES nonlinear function on $f: \mathbb{F} \to \mathbb{F}$ given by $f(x) = x^{(-1)}$, can be extended to give a function $\widehat{f}: \overline{\mathbb{F}} \to \overline{\mathbb{F}}$ of the projective line by setting $\widehat{f}|_{\mathbb{F}} = f$

and requiring that $\widehat{f}(\infty) = \infty$. However, this extended AES nonlinear function is almost identical to the geometric or projective transformation $\overline{f}: \overline{\mathbb{F}} \rightarrow \overline{\mathbb{F}}$ of the projective line given by $z \mapsto \frac{1}{z}$, differing only at the points 0 and ∞. Thus the natural geometrical setting for considering the AES nonlinear function would seem to be the projective line $\overline{\mathbb{F}}$, as the AES nonlinear function is almost identical to a geometrical transformation of this line.

More generally, projective geometries are higher dimensional versions of the projective line. The projective geometry $\mathrm{PG}(m-1, \mathbb{F})$ (or $\mathrm{PG}(m-1, |\mathbb{F}|)$) is the set of one-dimensional subspaces of the m-dimensional vector space $\mathbb{F}^m$ under the action of the group of linear transformations of $\mathbb{F}^m$. The $(m-1)$-dimensional subspaces of $\mathbb{F}^m$ are known as the *hyperplanes* of the projective geometry $\mathrm{PG}(m-1, \mathbb{F})$. Thus $\overline{\mathbb{F}} = \mathrm{PG}(1, \mathbb{F})$. Two projective geometries are *isomorphic* if there is mapping between them which is bijective both on the point sets and the hyperplane sets, and which also preserves incidence. Projective geometries are examples of more general structures known as designs [12]. In particular, the set D is a 2-(v, k, λ) *design* if D has v elements called *points*, a collection of subsets called *blocks* such that each block has k points and any two points are contained in exactly λ blocks. For example, the projective geometry $\mathrm{PG}(m-1, \mathbb{F})$ $(m > 2)$ is a 2–$(|\mathbb{F}|^m - 1, |\mathbb{F}|^{m-1} - 1, |\mathbb{F}|^{m-2} - 1)$ design in which the hyperplanes form the blocks. We later consider projective geometries over the field GF(2) and their associated designs when we discuss the differential properties of the AES inversion mapping in Section 4.

3 Group-theoretic Properties of AES Inversion

3.1 Introduction to the Group-theoretic Properties of a Cipher

It is has been shown that the round functions of the AES [8, 20] generate the alternating group on the state space of the AES [26]. Similar results have been demonstrated for other well-known block ciphers [24, 9, 25]. It is of course possible to construct block ciphers whose round functions generate the alternating or symmetric group, but are easy to attack by exploiting statistical properties of the block cipher [17]. However, the rationale given by these and other papers and others is that a block cipher whose round functions generate the symmetric or alternating group cannot be attacked by the type of algebraic method illustrated in [21].

The key-dependent non-linear transformations of the AES are based on the mappings $x \mapsto x^{(-1)} + k$ in some binary finite field $\mathbb{F}$, where $x^{(-1)}$ denotes x^{-1} for $x \neq 0$ and 0 for $x = 0$. It has been observed that constructing a block cipher with n-bit blocks by using such transformations as the round functions gives a very weak cipher, and a description of the cryptanalysis of such a block cipher comprising solely of AES-like transformations (modified "SHARK" with "n"$= 1$) using a technique called the interpolation attack has been given [14, 13]. The interpolation attack on such a block cipher is fundamentally an algebraic technique of the type supposedly excluded if the round functions generate the alternating or symmetric group on the state space. However, as we show below,

the set of such transformations generates the symmetric group on $\mathbb{F}$. This leads us to consider the nature of what exactly is meant by "the group generated by a cipher", and we conclude the Section with some comments on this issue. We note that some similar ideas were discussed in [7].

3.2 Groups generated by AES-like Transformations

We let $f_k: \mathbb{F} \to \mathbb{F}$ denote the function $x \mapsto x^{(-1)} + k$ for $k \in \mathbb{F}$, and we term such a transformation an *AES-like* transformation. It is clear that f_k is a permutation, so $f_k \in \mathrm{Sym}(\mathbb{F})$, the symmetry group of $\mathbb{F}$, where the group action of $\mathrm{Sym}(\mathbb{F})$ on the elements of $\mathbb{F}$ is defined in the usual way. Thus the set of AES-like transformations from $\mathbb{F}$ to $\mathbb{F}$ for one round is given by the set

$$S_{\mathbb{F}} = \{f_k: \mathbb{F} \to \mathbb{F} \mid f_k(x) = x^{(-1)} + k, k \in \mathbb{F}\}.$$

We are interested in the group generated by $S_{\mathbb{F}}$, which is a subgroup of $\mathrm{Sym}(\mathbb{F})$.

We contrast this set of transformations $S_{\mathbb{F}}$ with the set $S_{\overline{\mathbb{F}}}$ of *inversive-type* transformations from $\overline{\mathbb{F}}$ to $\overline{\mathbb{F}}$ defined by

$$S_{\overline{\mathbb{F}}} = \left\{\overline{f}_k: \overline{\mathbb{F}} \to \overline{\mathbb{F}} \mid \overline{f}_k(x) = x^{-1} + k, k \in \mathbb{F}\right\}.$$

By writing $x^{-1} + k$ as $\frac{kx+1}{x+0}$, we can see from Section 2 that every element of $S_{\overline{\mathbb{F}}}$ is a projective transformation, so $S_{\overline{\mathbb{F}}} \subset \mathrm{PGL}(2, \mathbb{F})$, acting on $\overline{\mathbb{F}}$ in the usual projective way.

The transformation $f_k \in S_{\mathbb{F}}$ and its corresponding transformation $\overline{f}_k \in S_{\overline{\mathbb{F}}}$ are however very similar (as was noted in Section 2 when $k = 0$). More formally, we can consider a restricted set $S_{\mathbb{F}^*}$ of AES-type transformations from $\mathbb{F}^*$ to $\mathbb{F}$ defined as

$$S_{\mathbb{F}^*} = \{f_k: \mathbb{F}^* \to \mathbb{F} \mid f_k(x) = x^{-1} + k, k \in \mathbb{F}\}.$$

The functions AES-like transformations in $S_{\mathbb{F}^*}$ are simply those in $S_{\mathbb{F}}$ with a restricted domain, whilst the inversive-type transformations in $S_{\mathbb{F}^*}$ are also simply those in $\overline{\mathbb{F}}$ with a restricted domain, Thus we have

$$S_{\mathbb{F}^*} = \{f_k|_{\mathbb{F}^*} \mid f_k \in S_{\mathbb{F}}\}. = \{\overline{f}_k|_{\mathbb{F}^*} \mid \overline{f}_k \in S_{\overline{\mathbb{F}}}\}.$$

It can thus be seen that an AES-like transformation f_k on $\mathbb{F}$ and its corresponding inversive-type transformation $\overline{f}_k$ on $\overline{\mathbb{F}}$ only differ for at most two elements of their domains (0 and ∞). However, this seemingly insignificant difference between the two corresponding transformations in $S_{\mathbb{F}}$ and $S_{\overline{\mathbb{F}}}$ give rise to a big difference in the groups generated by $S_{\mathbb{F}}$ and $S_{\overline{\mathbb{F}}}$. We thus now show that $S_{\mathbb{F}}$ generates (generally) the symmetric group, whereas $S_{\overline{\mathbb{F}}}$ generates a projective group. The relevant proofs are given in Appendix A.

We note that the related group $\langle x \mapsto x^{(-1)}, x \mapsto x + k\rangle$ was discussed in [7]. However, the group we consider, $\langle S_{\mathbb{F}}\rangle$, is generated by transformations closer to AES transformations than "inversion" and subkey addition considered separately. Moreover, Theorem 4.3.1 of [7], the analogous result to our Theorem 1, is incorrect.

We first consider the group generated by $S_{\overline{\mathbb{F}}}$, the set of inversive-type transformations of $\overline{\mathbb{F}}$. We can identify this set of projective transformations with a set $T = \eta(S_{\overline{\mathbb{F}}})$ of unimodular matrices, where $\eta\colon \mathrm{PGL}(2,\mathbb{F}) \to \mathrm{SL}(2,\mathbb{F})$ is the group isomorphism of Section 2. The following two results then show that $\langle S_{\overline{\mathbb{F}}} \rangle = \mathrm{PGL}(2,\mathbb{F})$.

Lemma 1. *The group generated by the set of matrices*

$$T = \left\{ \begin{pmatrix} k & 1 \\ 1 & 0 \end{pmatrix} \;\middle|\; k \in \mathbb{F} \right\}$$

is $SL(2,\mathbb{F})$, the group of all 2×2 matrices over $\mathbb{F}$ with determinant 1.

Corollary 1. *The group generated by the set $S_{\overline{\mathbb{F}}}$ of inversive-type transformations from $\overline{\mathbb{F}}$ to $\overline{\mathbb{F}}$ is $PGL(2,\mathbb{F})$ acting on $\overline{\mathbb{F}}$.*

We now consider the group generated by $S_{\mathbb{F}}$, the set of AES-like transformations of $\mathbb{F}$. The two smallest ($n \leq 2$) fields $\mathbb{F}$ of characteristic 2 are special cases. For $n = 1$, we have $\mathbb{F} = \mathrm{GF}(2)$ and $S_{\mathbb{F}} = \langle (0,1) \rangle = \mathrm{Sym}(\mathrm{GF}(2))$. For $n = 2$, we have $\mathbb{F} = \mathrm{GF}(2^2) = \{0, 1, \theta, \theta^2\}$ where $\theta^2 = \theta + 1$. Thus $S_{\mathbb{F}} = \{f_0, f_1, f_\theta, f_{\theta^2}\}$, and we summarise these permutations of $S_{\mathbb{F}}$ in the Table below.

Permutation	Mapping	Cycle Notation
f_0	$x \mapsto x^{(-1)}$	(θ, θ^2)
f_1	$x \mapsto x^{(-1)} + 1$	$(0, 1)$
f_θ	$x \mapsto x^{(-1)} + \theta$	$(0, \theta, 1, \theta^2)$
f_{θ^2}	$x \mapsto x^{(-1)} + \theta^2$	$(0, \theta^2, 1, \theta)$

We note that $f_0 = f_\theta^2 f_1$ and $f_{\theta^2} = f_\theta^{-1}$, so in fact $\langle S_{\mathbb{F}} \rangle = \langle f_1, f_\theta \rangle$. Furthermore, $f_\theta^4 = f_1^2 = (f_1^{-1} f_\theta f_1) f_\theta = 1$, so we have

$$\langle S_{\mathbb{F}} \rangle = \langle f_1, f_\theta \mid f_\theta^4 = f_1^2 = (f_1^{-1} f_\theta f_1) f_\theta = 1 \rangle.$$

This is the group presentation for the *dihedral* group D_8 with 8 elements ([2] Section 28.81), Thus, for $n = 2$, $S_{\mathbb{F}}$ generates the dihedral group D_8, rather than the symmetric group $Sym(\mathbb{F})$.

In the general case when $n > 2$, $\mathbb{F}$ has at least 8 elements. For this general case we associate a fractional linear transformation of $\overline{\mathbb{F}}$ with a permutation of $\mathbb{F}$ by means of an injective function

$$\Psi\colon \mathrm{PGL}(2,\mathbb{F}) \to \mathrm{Sym}(\mathbb{F}),$$

which is defined for $c = 0$ by

$$\left(x \mapsto \frac{ax+b}{cx+d} \right) \mapsto \left(x \mapsto \frac{ax+b}{cx+d} \right),$$

and is defined for $c \neq 0$ by

$$\left(x \mapsto \frac{ax+b}{cx+d} \right) \mapsto \left(x \mapsto \begin{cases} \frac{ax+b}{cx+d} & \text{for } x \neq \frac{d}{c} \\ \frac{a}{c} & \text{for } x = \frac{d}{c} \end{cases} \right).$$

By considering the elements $f_k \in S_{\mathbb{F}}$ and $\overline{f}_k \in S_{\overline{\mathbb{F}}}$ defined earlier, we can see that $\Psi(S_{\overline{\mathbb{F}}}) = S_{\mathbb{F}}$. Hence the set of generators of $\mathrm{PGL}(2, \mathbb{F})$ can be associated with the set of AES-like transformations. This association allows us to prove the following results which show that $\langle S_{\mathbb{F}} \rangle = \mathrm{Sym}(\mathbb{F})$.

Lemma 2. *The set $S_{\mathbb{F}}$ generates the transposition $(0, 1)$ of $\mathrm{Sym}(\mathbb{F})$.*

Lemma 3. *For $n > 2$, the set $S_{\mathbb{F}}$ generates a 2-transitive subgroup of $\mathrm{Sym}(\mathbb{F})$.*

Theorem 1. *For $n > 2$, the group generated by the set $S_{\mathbb{F}}$ of AES-like transformations from $\mathbb{F}$ to $\mathbb{F}$ is $\mathrm{Sym}(\mathbb{F})$ acting on $\mathbb{F}$.*

3.3 Comments on the "Group Generated by a Cipher"

We have discussed the group generated by the set of AES-like transformations acting on the state space $\mathbb{F}$ in a similar manner to the discussions given in [24, 9, 25, 26]. We have shown that the group generated by the AES-like transformations is generally the symmetric group on $\mathrm{Sym}(\mathbb{F})$. However, we can associate each AES-like transformation of $\mathbb{F}$ with an inversive-type transformation of $\overline{\mathbb{F}}$. A pair of such associated transformations give the same transformation on $\mathbb{F}$ unless a 0-inversion occurs. Moreover, 0-inversion is a rare event unless n is very small. Thus it seems that a very natural group action to consider for cryptanalytic purposes is that of the group generated by the set of inversive-type transformations acting on the projective line $\overline{\mathbb{F}}$. This group is $\mathrm{PGL}(2, \mathbb{F})$, which is generally ($n > 2$) much smaller and more structured than the group $\mathrm{Sym}(\mathbb{F})$ of AES-like transformations acting on the state space $\mathbb{F}$.

The discussion of the interpolation attack on a block cipher consisting of many rounds of iterated AES-like transformations (such as modified "SHARK" with with "n"$= 1$ [14, 13]) is straightforward in the context of the projective group. Except for 0-inversion, a round transformation is naturally considered as an element of $\mathrm{PGL}(2, \mathbb{F})$ acting on the projective line $\overline{\mathbb{F}}$. Thus this block cipher, which is the iteration of many such transformations, is also an element of $\mathrm{PGL}(2, \mathbb{F})$ unless a 0-inversion occurs. However, $\mathrm{PGL}(2, \mathbb{F})$ is a sharply triply transitive group ([23], Theorem 4.5.4), so if we know only three plaintext-ciphertext pairs (with no 0-inversion), then we can identify the unique element of $\mathrm{PGL}(2, \mathbb{F})$ corresponding to the encryption transformation. This should enable us to break the block cipher with three such pairs, though it has been stated that four such pairs are needed [14, 13, 1, 7].

It is clear that in discussing the "group generated by a cipher" there is always an accompanying group action on some set to consider. The above example clearly shows that the "obvious" group with the "obvious" implicit action on the state space may not be the most relevant "group generated by the cipher" when discussing the algebraic properties of that cipher. For practical purposes, we could have regarded an encryption transformation in the above example as an element of a small structured (projective) group acting on a slightly altered set rather than as a general permutation. It is this projective group that gives a

much better indication of this cipher's strength against certain types of algebraic attacks than the general symmetry group. It is thus clear from the above example that, when considering the group generated by a collection of block cipher round transformations, the set on which the transformations act has to be carefully chosen. There is a sense in the above construction in which the original state space $\mathbb{F}$ is embedded in a larger state space $\overline{\mathbb{F}} = \mathbb{F} \cup \{\infty\}$ with 0 and ∞ being identified when the embedding needs reversing. This is in many ways similar to the general ideas of embedding a block cipher state space algebra in a larger state space algebra discussed in [18, 6]. The interesting question when discussing the "group generated by the AES" is whether for the AES there is a similar construction to the above example for the AES state space $\mathbb{F}^{16}$ ($n = 8$), but which also gives a smaller and more structured group than the symmetric or alternating group on $\mathbb{F}^{16}$.

4 Differential Properties of AES Inversion

4.1 Introduction to the Differential or XOR Table

One of the standard techniques used to assess the security of a block cipher is that of differential cryptanalysis [3, 4]. We give a preliminary discussion of the differential properties of inversion mappings from a projective viewpoint. For a cryptographic function, the major tool used in differential cryptanalysis is the XOR or Difference Table. For a function $g\colon \mathbb{F} \to \mathbb{F}$, it is a $2^n \times 2^n$ table defined for $\alpha, \beta \in \mathbb{F}$ by

$$N_g(\alpha, \beta) = \#\{x \in \mathbb{F} \mid g(x + \alpha) + g(z) = \beta\}.$$

Thus $N_g(\alpha, \beta)$ measures the number of times an input difference of α is mapped to an output difference of β, so N_g can be used to calculate the probability that certain input differences propagate throughout the cipher. If the differences from round to round are regarded as a random process, the XOR Table (suitably normalised) is essentially the matrix of transition probabilities [15]. Some simple properties for the zero row or zero column are that $N_g(0, 0) = 2^n$ and $N_g(0, \beta) = 0$ for $\beta \neq 0$, with $N_g(\alpha, 0) = 0$ for $\alpha \neq 0$ if g is invertible. Furthermore, the row sum is given by $\sum_\beta N_g(\alpha, \beta) = 2^n$, whilst if g is invertible the column sum has the same property, that is $\sum_\beta N_g(\alpha, \beta) = 2^n$. The maximum value of this XOR Table (for $\alpha \neq 0$) gives an upper bound for the probability of difference propagation and so is clearly of interest. This idea is captured by the following definition [19].

Definition 1. $g\colon \mathbb{F} \to \mathbb{F}$ is *differentially δ-uniform* if for all $\alpha \neq 0$ and β,

$$\#\{x \in \mathbb{F} \mid g(x) + g(x + \alpha) = \beta\} \leq \delta.$$

Thus g is differentially δ-uniform if the maximum value of $N_g(\alpha, \beta)$ ($\alpha \neq 0$) is at most δ. Some further discussion of the differentially δ-uniform properties of

power mappings are given in [5]. Furthermore, according to the AES specifications [20, 8], the nonlinear function of AES ($x \mapsto x^{(-1)}$) of the AES was chosen partially because of the discussion of its properties given in [19].

In the remainder of this section, we consider the *Differential* or XOR Table of the AES nonlinear function $f: \mathbb{F} \to \mathbb{F}$ defined by $x \mapsto x^{(-1)}$. The differential properties of this AES nonlinear function in regard of the XOR Table give rise to a particular quadratic equation. Some properties of this particular quadratic equation have previously been considered in [11]. We therefore revisit this discussion of [11] before using these results to calculate $N_f(\alpha, \beta)$ and so completely characterise the XOR Table for the AES. This enables us to demonstrate some interesting connections between this AES XOR Table and projective geometry that arise from this characterisation.

4.2 Quadratic Equations over Fields of Even Characteristic

Section 1.4 of [11] gives the following discussion about solutions to quadratic equations of even characteristic (that is over $\mathbb{F}$). The *trace* of an element of $\mathbb{F}$ is defined to be the sum of its conjugates. Thus the trace mapping $\mathrm{Tr}: \mathbb{F} \to \mathrm{GF}(2)$ is defined by $x \mapsto x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$. As squaring is a field automorphism for a field of even characteristic, the trace mapping is a GF(2)-linear mapping, that is Tr is a linear transformation of $\mathbb{F}$ when $\mathbb{F}$ is considered as a vector space of dimension n over GF(2). The kernel of this linear transformation is a subspace of $\mathbb{F}$ (considered as a vector space) of dimension $n-1$. This kernel or subspace is denoted by $\mathcal{C}_0$ and called the set of elements of *category zero*, and its coset is denoted by $\mathcal{C}_1$ and called the set of elements of *category one*. Thus we have

$$\mathcal{C}_0 = \{x \in \mathbb{F} \mid \mathrm{Tr}(x) = 0\} \quad \text{and} \quad \mathcal{C}_1 = \{x \in \mathbb{F} \mid \mathrm{Tr}(x) = 1\}.$$

We then have the following results from Section 1.4 of [11].

Theorem 2. *Let the finite field $\mathbb{F}$ and categories $\mathcal{C}_0$ and $\mathcal{C}_1$ be defined as above.*

1. *$y^2 + y + \epsilon = 0$ has two solutions if $\epsilon \in \mathcal{C}_0$ and no solutions if $\epsilon \in \mathcal{C}_1$.*
2. *$0 \in \mathcal{C}_0$.*
3. *If n is even then $1 \in \mathcal{C}_0$, whereas if n is odd then $1 \in \mathcal{C}_1$.*
4. *$|\mathcal{C}_0| = |\mathcal{C}_1| = 2^{n-1}$.*

4.3 The XOR Table for AES Inversion

We now discuss the differential properties of the AES nonlinear transformation $f: \mathbb{F} \to \mathbb{F}$ defined by $f(x) = x^{2^n-2} = x^{(-1)}$. Thus we consider

$$\begin{aligned} N_f(\alpha, \beta) &= \{x \in \mathbb{F} \mid f(x) + f(x+\alpha) = \beta\} \\ &= \{x \in \mathbb{F} \mid x^{(-1)} + (x+\alpha)^{(-1)} = \beta\}. \end{aligned}$$

It has been shown that the AES inversion function is differentially 4-uniform (at worse) [19], and indeed the known results concerning N_f seem to be upper

bounds. We now calculate $N_f(\alpha, \beta)$ exactly for all $\alpha, \beta \in \mathbb{F}$, so we calculate the number of solutions of the equation

$$x^{(-1)} + (x + \alpha)^{(-1)} = \beta.$$

We have already noted that $N_f(0, 0) = 2^n$ and that $N_f(\alpha, 0) = N_f(0, \beta) = 0$ for $\alpha, \beta \neq 0$. We therefore assume that $\alpha, \beta \in \mathbb{F}^*$. The calculation of $N_f(\alpha, \beta)$ then splits into two cases depending on whether "AES-inversion" coincides with $\mathbb{F}$-inversion. Thus we define

$$\begin{aligned} N_1(\alpha, \beta) &= \#\{ \quad x \in \{0, \alpha\} \quad \mid x^{(-1)} + (x + \alpha)^{(-1)} = \beta \} \\ \text{and } N_2(\alpha, \beta) &= \#\{ x \in \mathbb{F} \setminus \{0, \alpha\} \mid \quad x^{-1} + (x + \alpha)^{-1} = \beta \quad \}, \end{aligned}$$

so $N_f(\alpha, \beta) = N_1(\alpha, \beta) + N_2(\alpha, \beta)$. We now consider these two cases.

Case 1: $N_1(\alpha, \beta)$.
In this case we have $x = 0$ or $x = \alpha$. In both cases, $x^{(-1)} + (x + \alpha)^{(-1)} = 0^{(-1)} + \alpha^{(-1)} = \alpha^{-1}$. Thus $x^{(-1)} + (x + \alpha)^{(-1)} = \beta$ has one solution if and only if $\alpha^{-1} = \beta$, or equivalently $\alpha\beta = 1$, and no solution otherwise. Therefore $N_1(\alpha, \beta) = 2$ if $\alpha\beta = 1$ and $N_1(\alpha, \beta) = 0$ otherwise.

Case 2: $N_2(\alpha, \beta)$.
In this case, we are considering solutions to the equation

$$\frac{1}{x} + \frac{1}{x + \alpha} = \frac{\alpha}{x^2 + \alpha x} = \beta,$$

which gives the quadratic equation $\beta x^2 + \alpha\beta x + \alpha = 0$ or the equivalent monic quadratic equation $x^2 + \alpha x + \frac{\alpha}{\beta} = 0$ for $x \neq 0, \alpha$. If we make the substitution $x = \alpha y$, then we can obtain the monic quadratic equation $y^2 + y + (\alpha\beta)^{-1} = 0$, so $N_2(\alpha, \beta) = \#\{y \in \mathbb{F} \mid y^2 + y + (\alpha\beta)^{-1} = 0\}$. However, the number of solutions of this quadratic equation was given in Theorem 2 of Section 4.2. Thus we have $N_2(\alpha, \beta) = 2$ if $\mathrm{Tr}((\alpha\beta)^{-1}) = 0$ and $N_2(\alpha, \beta) = 0$ if $\mathrm{Tr}((\alpha\beta)^{-1}) = 1$.

We can now combine the two cases to find $N_f(\alpha, \beta)$. With a slight abuse of notation, we can regard the trace mapping as an integer, so we have:

$$N_f(\alpha, \beta) = \begin{cases} 2^n & \text{if } \alpha = \beta = 0; \\ 0 & \text{if } \alpha\beta = 0 \text{ but not both zero;} \\ 2(1 - \mathrm{Tr}(1)) + 2 & \text{if } \alpha\beta = 1; \\ 2(1 - \mathrm{Tr}((\alpha\beta)^{-1}) & \text{if } \alpha\beta \neq 0, 1. \end{cases}$$

For the AES, $n = 8$ is even, which is a special case of the following result.

Theorem 3. *The values $N_f(\alpha, \beta)$ in the XOR Table for AES-like inversion are given for even n by:*

$$N_f(\alpha, \beta) = \begin{cases} 2^n & \textit{if } \alpha = \beta = 0; \\ 0 & \textit{if } \alpha\beta = 0 \textit{ but not both zero;} \\ 4 & \textit{if } \alpha\beta = 1; \\ 2 & \textit{if } \alpha\beta \neq 0, 1 \text{ and } \mathrm{Tr}\left((\alpha\beta)^{-1}\right) = 0; \\ 0 & \textit{if } \alpha\beta \neq 0, 1 \text{ and } \mathrm{Tr}\left((\alpha\beta)^{-1}\right) = 1. \end{cases}$$

4.4 The AES Inversion XOR Table and Projective Geometry

The XOR Table for a nonlinear function of a block cipher is mainly of interest as a tool for differential cryptanalysis. For the AES, we showed in Theorem 3 that the entries in the XOR Table for the AES are characterised mainly by the Trace mapping. However, we can also define certain geometric structures and associated ideas in terms of the Trace mapping. Thus we show in this Section that the AES XOR Table naturally defines a projective geometry.

We can remove the row corresponding to $\alpha = 0$ and the column corresponding to $\beta = 0$, and call the resulting $(2^n - 1) \times (2^n - 1)$ table the *Reduced AES XOR Table*. The underlying condition of this Reduced AES XOR Table is that $N_f(\alpha, \beta) = 2$ when $\mathrm{Tr}((\alpha\beta)^{-1}) = 0$ with a correction for 0-inversion. However, we can use this trace condition, and hence also the AES XOR Table, to construct the following incidence structure based on the multiplicative group $\mathbb{F}^*$ of the finite field $\mathbb{F}$. Thus suppose D is the structure consisting of the elements of $\mathbb{F}^*$ as points and the subsets

$$B_\alpha = \{\beta \in \mathbb{F}^* \mid \mathrm{Tr}((\alpha\beta)^{-1}) = 0\} \qquad (\alpha \in \mathbb{F}^*),$$

as blocks. We can also use Theorem 3 to define D directly from the XOR Table, when the blocks can also be defined for $\alpha \in \mathbb{F}^*$ by

$$B_\alpha = \begin{cases} \{\beta \in \mathbb{F}^* \mid N_f(\alpha, \beta) \geq 2\} & n \text{ even} \\ \{\beta \in \mathbb{F}^* \mid N_f(\alpha, \beta) = 2\} \setminus \{\alpha^{-1}\} & n \text{ odd.} \end{cases}$$

Hence the Reduced XOR Table gives the incidence matrix for the structure D.

Suppose we now order the rows and columns of the Reduced XOR Table $1, \rho, \rho^2, \ldots, \rho^{2^n-2}$, where ρ is a primitive element of $\mathbb{F}$, then the sequence

$$\mathrm{Tr}\left(\alpha^{-1}(\rho^{-1})^0\right), \mathrm{Tr}\left(\alpha^{-1}(\rho^{-1})^1\right), \ldots, \mathrm{Tr}\left(\alpha^{-1}(\rho^{-1})^{2^n-2}\right)$$

is an m-sequence (as ρ^{-1} is primitive [16]) whose minimal polynomial is the minimal polynomial of ρ^{-1}. Thus the rows of the Reduced XOR Table for the nonlinear function of the AES are essentially all m-sequences with the same minimal polynomial, and so are shifts of one another. However, there is a detailed discussion given in [10] about the equivalence of the incidence structure defined from a binary m-sequence and the projective geometry $\mathrm{PG}(n-1, 2)$ over the field GF(2). Furthermore, this equivalence is made explicit by using the trace function Tr discussed above. Thus from [10] we have the following result.

Theorem 4. *The projective geometry $PG(n-1, 2)$ is isomorphic to the incidence structure D defined from the Reduced AES XOR Table.*

The points of the projective geometry $\mathrm{PG}(n-1, 2)$ of Theorem 4 are the elements of $\mathbb{F}^*$ and the hyperplanes are the sets B_α ($\alpha \in \mathbb{F}^*$) defined above. Theorem 4 also shows that the incidence structure D is a 2-design.

In summary, we have shown that the Reduced XOR Table for AES inversion, interpreted in a very natural way as an incidence matrix, gives a projective geometry. Thus we have not only characterised the entries $N_f(\alpha, \beta)$ of the AES XOR Table, but we have also shown that this AES XOR Table is fundamentally a projective geometry.

4.5 Comments on the AES XOR Table from a Projective Viewpoint

The projective techniques used in this Section may be able to adapted to some other functions other than the AES inversion mapping, for example certain power maps. Thus, for example, conjugates of the AES inversion mapping, such as $x \mapsto (x^{(-1)})^2$, would give essentially the same results as the AES inversion.

The projective viewpoint has allowed us, in particular, to demonstrate certain geometric properties of the AES XOR Table for an individual AES inversion. However, for these AES differential geometric properties to be of interest for cryptanalysis, we would need to combine these results for a single inversion for several inversions both within the same round and across several rounds. Of course, calculating the XOR Table for the simultaneous application of the AES inversion within one round is straightforward. We simply multiply the individual $N_f(\alpha, \beta)$ values for each AES inversion, and it is clear that to maximise the overall value we need as many inputs (α) to be non-zero as possible. Calculating a specific entry in the global XOR Table across several rounds would seem much more problematical. One of the AES's main design features is the "wide-trail" strategy [8], which (in some sense) maximises the number of non-zero differential inputs used and so would seem to ensure that a specific entry in the global XOR Table is both small and difficult to calculate. However, the set of non-zero entries in the XOR Table across one round do form some sort of coherent geometrical structure in some space. It is conceivable that it might be possible to analyse the effect of linear diffusion on this geometrical structure and so formulate some type of analysis of the differential properties of the AES based on the underlying geometrical structure.

5 Conclusions

The geometrical properties of the AES inversion function that we have discussed in this paper are not shared, as far as we are aware, by other well-known block ciphers (except those based on the AES). Thus the geometrical properties of the AES nonlinear function seem to be fundamentally unique to the AES.

The properties we have been discussing have generally referred to a single AES inversion. The challenge, as discussed in both Sections 3 and 4, is to find some way of combining such properties for several AES inversions, that is of combining the underlying projective structures of each individual AES inversion. However, the rich geometrical structure of AES inversions clearly merits further investigation.

References

1. K. Aoki and S. Vaudenay. On the use of GF-Inversion as a Cryptographic Primitive. In *Selected Areas in Cryptography (SAC) 2003*, volume 3006 of *LNCS*, pages 234–347. Springer-Verlag, 2004.
2. M. Aschbacher. *Finite Group Theory.* Cambridge University Press, 1986.

3. E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In A.J. Menezes and S.A. Vanstone, editors, *Advances in Cryptology - CRYPTO 90*, volume 537 of *LNCS*, pages 1–21. Springer-Verlag, 1991.
4. E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, 4:3–72, 1991.
5. A. Canteaut. Differential Cryptanalysis of Feistel Ciphers and Differentially δ-uniform mappings. *Selected Areas in Cryptography (SAC) 1997*, 1997.
6. C. Cid, S. Murphy, and M. J. B. Robshaw. An Algebraic Framework for Cipher Embeddings . In *10th IMA International Conference on Coding and Cryptography*, LNCS. Springer-Verlag, 2005. To appear.
7. N.T. Courtois. The Inverse S-Box, Non-linear Polynomial Relations and Cryptanalysis of Block Ciphers. In V. Rijmen H. Dobbertin and A. Sowa, editors, *Advanced Encryption Standard - AES: Fourth International Conference*, volume 3373 of *LNCS*, pages 234–347. Springer-Verlag, 2005.
8. J. Daemen and V. Rijmen. *The Design of Rijndael*. Springer-Verlag, 2002.
9. W. Stephan G. Hornauer and R. Wernsdorf. Markov Ciphers and Alternating Groups. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT 93*, volume 765 of *LNCS*, pages 453–460. Springer-Verlag, 1994.
10. R. A. Games. The geometry of m-sequences: Three valued cross correlations and quadrics in finite projective geometry. *SIAM J. Alg. Disc. Meth.*, 17:42–52, 1986.
11. J. W. P. Hirschfeld. *Projective Geometry over Finite Fields*. Oxford Mathematical Monographs, 1998.
12. D. R. Hughes and F. C. Piper. *Design Theory*. Cambridge University Press, 1985.
13. T. Jakobsen and L. Knudsen. Attacks on Block Ciphers of low Algebraic Degree. *Journal of Cryptology*, 14:197–210, 2001.
14. T. Jakobsen and L. R. Knudsen. The Interpolation Attack on Block Ciphers. In E. Biham, editor, *Fast Software Encryption – FSE97*, volume 1267 of *LNCS*, pages 28–40. Springer, 1997.
15. X. Lai, J. L. Massey, and S. Murphy. Markov Ciphers and Differential Cryptanalysis. In D.W. Davies, editor, *Advances in Cryptology - EUROCRYPT 91*, volume 547 of *LNCS*, pages 17–38. Springer-Verlag, 1991.
16. R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications*. Cambridge University Press, 1994.
17. S. Murphy, K. Paterson, and P. Wild. A Weak Cipher that Generates the Symmetric Group. *Journal of Cryptology*, 7:61–65, 1994.
18. S. Murphy and M. J. B. Robshaw. Essential algebraic structure within the AES. In M. Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *LNCS*, pages 1–16. Springer-Verlag, 2002.
19. K. Nyberg. Differentially Uniform Mappings for Cryptography. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT 93*, volume 765 of *LNCS*, pages 55–64. Springer-Verlag, 1994.
20. National Institute of Standards and Technology. Federal Information Processing Standards Publication (FIPS) 197: The Advanced Encryption Standard. 26 November 2001.
21. K. Paterson. Imprimitive permutation groups and trapdoors in iterated block ciphers. In L.R. Knudsen, editor, *Fast Software Encryption*, volume 1636 of *LNCS*, pages 201–214. Springer-Verlag, 1999.
22. J.J. Rotman. *Theory of Groups*. Wm. C. Brown Publishers, 1988.
23. T. Tsuzuku. *Finite Groups and Finite Geometries*. Cambridge Unversity Press, 1976.

24. R. Wernsdorf. The One-Round Functions of the DES Generate the Alternating Group. In R.A. Rueppel, editor, *Advances in Cryptology - EUROCRYPT 92*, volume 658 of *LNCS*, pages 99–112. Springer-Verlag, 1993.
25. R. Wernsdorf. IDEA, SAFER++ and Their Permutation Groups. *Second NESSIE Workshop*, 2001.
26. R. Wernsdorf. The round functions of rijndael generate the alternating group. In J. Deamen and V. Rijmen, editors, *Fast Software Encryption - FSE02*, volume 2365 of *LNCS*, pages 143–148. Springer, 2002.

A Group–Theoretic Proofs

Lemma 1. *The group generated by the set of matrices*

$$T = \left\{ \begin{pmatrix} k & 1 \\ 1 & 0 \end{pmatrix} \;\middle|\; k \in \mathbb{F} \right\}$$

is SL$(2, \mathbb{F})$*, the group of all* 2×2 *matrices over* $\mathbb{F}$ *with determinant* 1*.*

Proof. Every matrix in T has determinant 1, so $\langle T \rangle \leq \mathrm{SL}(2, \mathbb{F})$. Now, a matrix in $\mathrm{SL}(2, \mathbb{F})$ can be expressed as a product of matrices in T in the following way.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{cases} \begin{pmatrix} a(1+b) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} d & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} & \text{for} \quad c = 0; \\ \begin{pmatrix} \frac{1+a}{c} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1+d}{c} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \text{for} \quad c \neq 0. \end{cases}$$

Thus any matrix in $\mathrm{SL}(2, \mathbb{F})$ can be generated by elements in T.

Lemma 2. *The set* $S_{\mathbb{F}}$ *generates the transposition* $(0, 1)$ *of Sym*$(\mathbb{F})$*.*

Proof. The transformation $\overline{f}_1 \in \mathrm{PGL}(2, \mathbb{F})$ defined by $(x \mapsto \frac{1}{x} + 1)$ is represented by the matrix $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, which satisfies $A^3 = I$. We note that $\overline{f}_1$ permutes the elements of $\mathbb{F} \setminus \{0, 1\}$ as $\overline{f}_1 \colon \infty \mapsto 1 \mapsto 0 \mapsto \infty$.

We now consider the corresponding transformation $f_1 = \Psi(\overline{f}_1) \in S_{\mathbb{F}}$, defined by $x \mapsto x^{(-1)} + 1$. We note that $f_1 \colon 0 \mapsto 1 \mapsto 0$, so f_1 permutes the elements of $\mathbb{F} \setminus \{0, 1\}$ and furthermore f_1 and $\overline{f}_1$ are the same transformation on $\mathbb{F} \setminus \{0, 1\}$. Thus the triple iteration $f_1 f_1 f_1 \in \langle S_{\mathbb{F}} \rangle$ is therefore the identity on $\mathbb{F} \setminus \{0, 1\}$ and transposes 0 and 1. Hence the transposition $(0, 1) \in \langle S_{\mathbb{F}} \rangle$.

Lemma 3. *For* $n > 2$*, the set* $S_{\mathbb{F}}$ *generates a 2-transitive subgroup of Sym*$(\mathbb{F})$*.*

Proof. We first show that for any $p', q' \in \mathbb{F}$, the set $S_{\mathbb{F}}$ generates a permutation which maps p' to 0 and q' to 1. As the identity permutation performs this function for the trivial case, we assume that $(p', q') \neq (0, 1)$.

For ease of notation, we define $p, q \in \mathbb{F}$ such that $p' = p^2$ and $q' = q^2$. Now, the three transformations $\overline{f}_{\frac{p+q+p^2}{(p+q)^2}}, \overline{f}_{p+q}, \overline{f}_{\frac{1}{p+q}} \in \mathrm{PGL}(2, \mathbb{F})$ are given by

$$x \mapsto \frac{1}{x} + \frac{p+q+p^2}{(p+q)^2}\ ,\ \ x \mapsto \frac{1}{x} + (p+q) \text{ and } x \mapsto \frac{1}{x} + \frac{1}{p+q}$$

respectively. It can thus be shown from their corresponding matrices (or proof of Lemma 1) that their composition $\overline{h} \in \mathrm{PGL}(2, \mathbb{F})$ is given by

$$x \mapsto \frac{\frac{1}{p+q}x + \frac{p^2}{p+q}}{p+q} = \frac{x+p^2}{(p+q)^2},$$

so clearly $\overline{h}(p^2) = 0$ and $\overline{h}(q^2) = 1$. The composition h of the corresponding functions $f_{\frac{p+q+p^2}{(p+q)^2}}$, f_{p+q} and $f_{\frac{1}{p+q}}$ in $S_{\mathbb{F}}$ is clearly in $\langle S_{\mathbb{F}} \rangle$ and satisfies $h(p^2) = 0$ and $h(q^2) = 1$ unless a 0-inversion occurs. For the composition of these three functions, a 0-inversion occurs when evaluating inputs of 0 or $p+q$, when $h(0) = \frac{p^2}{(p+q)^2}$ and $h(p+q) = \frac{p+q+p^2}{(p+q)^2}$. An input of 0 occurs when either $p^2 = 0$ or $q^2 = 0$, whereas an input of $p+q$ occurs when either $p^2 = p+q$ or $q^2 = p+q$. For this latter input of $p+q$, we can deduce that if $p^2 = p+q$ then $q^2 = p^2(1+p)^2$ and similarly if $q^2 = p+q$ then $p^2 = q^2(1+q)^2$. Thus we can identify four special cases for (p^2, q^2), namely $(0, q^2)$, $(p^2, 0)$, $(p^2, p^2(1+p)^2)$ and $(q^2(1+q)^2, q^2)$, and except for these four special cases, the above permutation maps p^2 to 0 and q^2 to 1. We now consider these four special cases.

1. *Permutation mapping* 0 *to* 0 *and* q^2 *to* 1.
   The permutation $x \mapsto x^{(-1)} + \lambda^2$ maps 0 to λ^2 and q^2 to $\frac{(1+\lambda q)^2}{q^2}$. We know that there exists a permutation mapping λ^2 to 0 and $\frac{(1+\lambda q)^2}{q^2}$ to 1, except possibly for the four special cases given above. These four special cases are given by:
   (a) $\lambda^2 = 0$;
   (b) $\frac{(1+\lambda q)^2}{q^2} = 0$ so $\lambda^2 = \frac{1}{q^2}$;
   (c) $\lambda^2 = \lambda + \frac{1+\lambda q}{q} = \frac{1}{q}$;
   (d) $\frac{(1+\lambda q)^2}{q^2} = \lambda + \frac{1+\lambda q}{q} = \frac{1}{q}$ which gives $1 + q^2\lambda^2 = q$ so $\lambda^2 = \frac{q+1}{q^2}$.
   Thus there may not exist a permutation mapping λ^2 to 0 and $\frac{(1+\lambda q)^2}{q^2}$ to 1 for the four special cases given by $\lambda^2 = 0, \frac{1}{q^2}, \frac{1}{q}, \frac{q+1}{q^2}$. However, for $n > 2$, $\mathbb{F}$ is a field with more than four elements, so we can always find a λ which is not one of these four special cases. Thus for $n > 2$ we can always find a permutation mapping λ^2 to 0 and $\frac{(1+\lambda q)^2}{q^2}$ to 1, and hence for $n > 2$ we can always find a permutation in $\langle S_{\mathbb{F}} \rangle$ mapping 0 to 0 and q^2 to 1.
2. *Permutation mapping* p^2 *to* 0 *and* 0 *to* 1.
   Using Part 1, there exists a permutation mapping p^2 to 1 and 0 to 0. However, the permutation of $\mathbb{F}$ given by $x \mapsto x^{(-1)} + 1$ maps 0 to 1 and vice versa. Thus there exists a permutation in $\langle S_{\mathbb{F}} \rangle$ mapping p^2 to 0 and 0 to 1.

3. *Permutation mapping* p^2 *to* 0 *and* $p^2(1+p)^2$ *to* 1 $(p \neq 0, 1)$.
   The permutation $x \mapsto x^{(-1)} + \frac{1}{p^2}$ maps p^2 to 0 and $p^2(1+p)^2$ to $\frac{1}{(1+p)^2}$, and using Part 1 there exists a permutation mapping 0 to 0 and $\frac{1}{(1+p)^2}$ to 1. Thus there exists a permutation in $\langle S_{\mathbb{F}} \rangle$ mapping p^2 to 0 and $p^2(1+p)^2$ to 1.
4. *Permutation mapping* $q^2(1+q)^2$ *to* 0 *and* q^2 *to* 1 $(q \neq 0, 1)$.
   By Part 3 there is a permutation mapping $q^2(1+q)^2$ to 1 and q^2 to 0, and as above the permutation $x \mapsto x^{(-1)} + 1$ maps 0 to 1 and vice versa, so there exists a permutation in $\langle S_{\mathbb{F}} \rangle$ mapping $q^2(1+q)^2$ to 0 and q^2 to 1.

In summary, have shown that for a given p', q', there exists a permutation $h_{p',q'} \in \langle S_{\mathbb{F}} \rangle$ mapping p' to 0 and q' to 1. Thus the permutation $h^{-1}_{p'',q''} h_{p',q'} \in \langle S_{\mathbb{F}} \rangle$ maps p' to p'' and q' to q''. Hence $\langle S_{\mathbb{F}} \rangle$ is a 2-transitive subgroup of $\mathrm{Sym}(\mathbb{F})$.

Theorem 1. *For* $n > 2$*, the group generated by the set* $S_{\mathbb{F}}$ *of AES-like transformations from* $\mathbb{F}$ *to* $\mathbb{F}$ *is Sym*$(\mathbb{F})$ *acting on* $\mathbb{F}$*.*

Proof. The group $\langle S_{\mathbb{F}} \rangle$ generated by the AES-like transformations contains the transposition $(0, 1)$ and is a 2-transitive subgroup of $\mathrm{Sym}(\mathbb{F})$. Thus $\langle S_{\mathbb{F}} \rangle$ contains all transpositions and so generates $\mathrm{Sym}(\mathbb{F})$ ([2] Section 15.4).