A note on an infeasible linearization of some block ciphers

Riccardo Aragona*[1], Anna Rimoldi†[1], and Massimiliano Sala‡[1]

[1]Department of Mathematics, University of Trento, Italy

Abstract

A block cipher can be easily broken if its encryption functions can be seen as linear maps on a small vector space. Even more so, if its round functions can be seen as linear maps on a small vector space. We show that this cannot happen for the AES. More precisely, we prove that if the AES round transformations can be embedded into a linear cipher acting on a vector space, then this space is huge-dimensional and so this embedding is infeasible in practice. We present two elementary proofs.

Keywords: AES, block cipher, group theory.

1 Introduction

The Advanced Encryption Standard (AES) [10] is nowadays the most widespread block cipher in commercial applications. It represents the state-of-the-art in block cipher design and the only known attack on its full version is the biclique attack [4], which still requires an amount of cryptanalytic effort slightly less than the brute-force key-search. Practical attacks on reduced versions of the AES only tackle up to 6 rounds, with the Partial Sum attack being the most dangerous [8, 1] The best that a designer can hope for a block cipher is that all its encryption functions behave in an unpredictable way (close to random), in particular the designer aims at a cipher behaviour totally different from linear or affine maps.
An indication of the cryptographic strength of the AES is that nobody has been able to show that its encryption functions are any closer to linear maps than arbitrary random functions. However, it might be possible to extend the AES to act on larger spaces, in such a way that the possible non-random behaviour of the AES becomes easier to spot. Generally speaking, the worst scenario for a designer consists of a space large enough to make the AES linear but small enough to allow practical computations.

In this note we prove in two elementary ways, respectively using counting arguments (Section 3) and number theory arguments (Section 4), that the round functions of the AES cipher cannot be embedded into a linear group acting on a vector space W, unless the dimension of W is huge, making this embedding useless in practice. Both proofs show that the smallest degree of a (faithful) representation of the group generated by the round functions of the AES, that is $\mathrm{Alt}((\mathbb{F}_2)^{128})$ [12], is at least 2^{67}.

*ric.aragona@gmail.com
†anna.rimoldi@gmail.com
‡maxsalacodes@gmail.com

Since computing a $2^{67} \times 2^{67}$ matrix is infeasible in practice, our result shows that this attack cannot be mounted in practice.

In 1976 Wagner [14] studied the (faithful) linear representations of $\mathrm{Alt}((\mathbb{F}_2)^{128})$ and was already able to prove that their minimal degree is 2^{128}. Therefore, we do not claim any new algebraic result in this note. The interest of our note lies in three facts. First, we provide elementary proofs of our degree estimate, lacking a deep algebraic background, while Wagner's proof follows an involved argument relying on representation theory. Second, we show the link between a purely group theory result and a possible practical application in cryptanalysis, providing thus more assurance in the cipher itself (since the attack cannot be practically mounted). Third, our two proofs are based on utterly different arguments, one counting the number of group elements and the other estimating the maximal element order, but do lead to the same numerical estimate, which we find unexpected and deserves noting.

This note is part of the PhD thesis of the second author [11], which was never before published in a peer-reviewed journal.

2 Preliminaries

Let $n \geq 2$ be an integer. Let $\mathbb{F} = \mathbb{F}_2$ be the field with 2 elements. Let $V = \mathbb{F}^n$ be the vector space over $\mathbb{F}$ of dimension n. We denote by $\mathrm{Sym}(V)$ and $\mathrm{Alt}(V)$, respectively, the symmetric and alternating group on V. We denote by $\mathrm{GL}(V)$ the group of all linear permutations of V.

Let $\mathcal{C}$ be any block cipher such that the plaintext space $\mathcal{M}$ coincides with the ciphertext space. Let $\mathcal{K}$ be the key space. Any key $k \in \mathcal{K}$ induces a permutation τ_k on $\mathcal{M}$. Since $\mathcal{M}$ is usually $V = \mathbb{F}^n$ for some $n \in \mathbf{N}$, we can view τ_k as an element of $\mathrm{Sym}(V)$. We denote by $\Gamma = \Gamma(\mathcal{C})$ the subgroup of $\mathrm{Sym}(V)$ generated by all the τ_k's. Unfortunately, the knowledge of $\Gamma(\mathcal{C})$ is out of reach for the most important block ciphers, such as the AES [10] and the DES [9]. However, researchers have been able to compute another related group. Suppose that $\mathcal{C}$ is the composition of l rounds (the division into rounds is provided in the document describing the cipher). Then any key k would induce l permutations, $\tau_{k,1}, \ldots, \tau_{k,l}$, whose composition is τ_k. For any round h, we can consider $\Gamma_h(\mathcal{C})$ as the subgroup of $\mathrm{Sym}(V)$ generated by the $\tau_{k,h}$'s (with k varying in $\mathcal{K}$). We can thus define the group $\Gamma_\infty = \Gamma_\infty(\mathcal{C})$ as the subgroup of $\mathrm{Sym}(V)$ generated by all the Γ_h's. Obviously, $\Gamma \leq \Gamma_\infty$. The group Γ_∞ is traditionally called the *group generated by the round functions* with independent sub-keys. This group is known for some important ciphers, for the AES we have

Proposition 1 ([12])**.**

$$\Gamma_\infty(\mathrm{AES}) = \mathrm{Alt}(\mathbb{F}^{128}).$$

Remark 1. *The fact that Γ_∞ is the alternating group is not an exception holding only for the AES. Indeed, any block cipher built choosing accurately the cipher components (SBoxes and linear mixing layer) will have Γ_∞ as either the alternating group or the symmetric group, even if the cipher is defined over a positive characteristic (see [5, 2]).*

Given a finite group G, we say that G can be *linearized* if there is an injective morphism $\pi : G \to \mathrm{GL}(W)$, for some vector space W (this is called a "faithful representation" in representation theory). If G can be linearized, then, for any element $g \in G$, an attacker can compute a matrix M_g corresponding to the action of g over W (via π). If the dimension of W is sufficiently small, the matrix computation is straightforward, since it is enough to evaluate g on a basis of W. In cryptanalysis, this attack would be called a *chosen-plaintext attack* and can easily be translated into a *known-plaintext attack* by collecting enough random plaintext-ciphertext pairs.

In this note we show that it is impossible to view $\Gamma_\infty(\mathrm{AES})$ as a subgroup of $\mathrm{GL}(W)$ with W of small dimension. In Cryptography it is customary to present estimates as powers of two, so our problem becomes to find the smallest m such that $\Gamma_\infty(\mathrm{AES})$ can be linearized in $\mathrm{GL}(\mathbb{F}^{2^m})$.

There are two elementary ways to show that a finite group H cannot be contained (as isomorphic image) in a finite group G. The first is to show that $|H| > |G|$, the second is to show that there is $\eta \in H$ such that its order is strictly larger than the maximum element order in G. In Section 3 we present our result using the first approach and we show that $m \geq 67$. In Section 4 we present our result using the second approach and we show again that $m \geq 67$.

3 Counting the group size

In this section we show that the order of $\mathrm{Alt}(\mathbb{F}^{128})$ is strictly larger than the order of $\mathrm{GL}(\mathbb{F}^{2^{66}})$, so that if $\mathrm{Alt}(\mathbb{F}^{128}) < \mathrm{GL}(\mathbb{F}^{2^m})$ then $m \geq 67$.
First we recall some well-known formulae: if $V = \mathbb{F}^n$,

$$|\mathrm{Sym}(V)| = 2^n!, \quad |\mathrm{Alt}(V)| = \frac{2^n!}{2} \quad |\mathrm{GL}(V)| = \prod_{h=0}^{n-1}(2^n - 2^h) < 2^{n^2}.$$

We begin with showing a lemma.

Lemma 1. *The following inequality holds*

$$2^{(2^7)^{19}} < 2^{128}! < 2^{(2^7)^{20}}.$$

Proof. Let $n = 2^7$, we have to show $2^{n^{19}} < 2^n! < 2^{n^{20}}$.
We first show that $2^{n^{19}} < 2^n!$.
Note that the following inequality

$$\frac{1}{2^{n-i}} \geq \frac{1}{2^{n-i+1} - h} \tag{1}$$

holds for $1 \leq i \leq n-2$ and $1 \leq h \leq 2^{n-i}$.
Clearly

$$\begin{aligned} 2^n! > 2^{n^{19}} \quad &\iff \quad 2^n(2^n-1)! > 2^n \cdot 2^{n^{19}-n} \\ &\iff \quad (2^n-1)(2^n-2)! > 2^{n^{19}-n} \cdot \frac{2^n-1}{2^n-1} \quad . \end{aligned}$$

We apply (1) with $i = 1$ and $h = 1$ and so we must prove

$$(2^n-1)(2^n-2)! > 2^{n^{19}-n} \cdot \frac{2^n-1}{2^{n-1}},$$

i.e.

$$(2^n-2)! > 2^{n^{19}-n-(n-1)}. \tag{2}$$

In a similar way for $i = 1$ and $h = 2$, from (2) we obtain

$$(2^n-2)(2^n-3)! > 2^{n^{19}-n-(n-1)} \cdot \frac{2^n-2}{2^{n-1}},$$

hence

$$2^n! > 2^{n^{19}} \iff (2^n-3)! > 2^{n^{19}-n-2(n-1)},$$

and so on for all $3 \leq h \leq 2^{n-1}$ we obtain that we must verify

$$(2^{n-1}-1)! > 2^{n^{19}-n-2^{n-1}(n-1)}.$$

Then we proceed by applying (1) for all $2 \leq i \leq n-2$ and all $1 \leq h \leq 2^{n-i}$, so that we need only to prove

$$(2^{n-(n-1)}-1)! \geq 2^{n^{19}-n-\sum_{i=1}^{n-1} 2^{n-i}(n-i)}.$$

In other words, we have to prove

$$1 > 2^{n^{19}-n-\sum_{i=1}^{n-1} 2^{n-i}(n-i)}, \quad \text{that is,} \quad 0 > n^{19} - n - \sum_{i=1}^{n-1} 2^{n-i}(n-i). \tag{3}$$

But a direct check shows that the right-hand size of (3) holds when $n = 2^7$.

We are left with proving the following inequality: $2^n! < 2^{n^{20}}$.
We proceed by induction for $2 \leq n \leq 2^7$. In this range a computer computation shows that

$$n^{20} + 2^n n + 2^n < (n+1)^{20}. \tag{4}$$

When $n = 2$, we have $2^2! < 2^{2^{20}}$.
Suppose that $2^n! < 2^{n^{20}}$ and $n \leq 2^7$. We have to prove that $2^{(n+1)}! < 2^{(n+1)^{20}}$. Since $2^{n+1}! = (2^n \cdot 2)! = 2^n!(2^n+1)\cdots(2^n+2^n)$ and since $2^n + j \leq 2^{n+1}$ for all $1 \leq j \leq 2^n$, we have

$$2^n!(2^n+1)\cdots(2^n+2^n) < 2^{n^{20}+n+1}\cdot(2^n+2)\cdots(2^n+2^n) \leq 2^{n^{20}+2^n(n+1)} = 2^{n^{20}+2^n n+2^n}$$

and, applying (4), we get $2^{n^{20}+2^n n+2^n} < 2^{(n+1)^{20}}$. Then the claimed inequality $2^{n+1}! < 2^{(n+1)^{20}}$ follows. □

Our result is contained in the following proposition.

Proposition 2. *Let $W = \mathbb{F}^{2^m}$ with $m \geq 2$. If $G < \mathrm{GL}(W)$, with G isomorphic to $\mathrm{Alt}(\mathbb{F}^{128})$, then $m \geq 67$.*

Proof. If $G < \mathrm{GL}(W)$, then $|G| \leq |\mathrm{GL}(W)|$. But $|\mathrm{Sym}(\mathbb{F}^{128})| = 2^{128}! > 2^{2^{133}}$ thanks to Lemma 1 and so

$$|G| = |\mathrm{Alt}(\mathbb{F}^{128})| = \frac{|\mathrm{Sym}(2^{128})|}{2} > \frac{2^{2^{133}}}{2} = 2^{2^{133}-1} > 2^{2^{132}} = 2^{(2^{66})^2} > |\mathrm{GL}(\mathbb{F}^{2^{66}})|.$$

□

Remark 2. *We could improve the previous bound to $l \geq 68$ by using the finite version of the Stirling formula:*

$$n\log_2(n) - n\log_2(e) \leq \log_2(n!) \leq n\log_2(n) - n\log_2(e) + \log_2(n),$$

or equivalently

$$\left(\frac{n}{e}\right)^n \leq n! \leq n\left(\frac{n}{e}\right)^n. \tag{5}$$

However, our proof involves only elementary combinatorial arguments, which are not enough to prove (5), since the latter requires some non-algebraic arguments, such as mathematical analysis.

4 Computing the maximum order of elements

In this section we compare the maximum order of elements in the two groups $\mathrm{Alt}(\mathbb{F}^{128})$ and $\mathrm{GL}(\mathbb{F}^{2^m})$. We use permutations of even order. We denote by $\mathrm{o}(\sigma)$ the order of any permutation σ.
We need the following two theorems.

Theorem 1 ([6]). *Let $\sigma \in \mathrm{GL}(\mathbb{F}^N)$, with $\mathrm{o}(\sigma)$ even and $N \geq 4$. Then*

$$\mathrm{o}(\sigma) \leq 2(2^{N-2} - 1) = 2^{N-1} - 2.$$

Moreover, there is $\sigma \in \mathrm{GL}(\mathbb{F}^N)$ whose order attains the upper bound.

Proof. It follows directly from Theorem 1 in [6], with $p = q = 2$ and $N \geq 4$ (so point (a) and (b) do not apply). □

Theorem 2 (Theorem 5.1.A at p. 145 in [7]). *Let $\nu \geq 3$ and $n = 2^\nu$. Then $\mathrm{Alt}(\mathbb{F}^\nu)$ contains an element η of order (strictly) greater than $e^{\sqrt{(1/4)n \ln n)}}$.*

In order to be able to compare the two estimates coming from Theorem 1 and Theorem 2, we rewrite Theorem 2 as follows, in order to have $\mathrm{o}(\sigma)$ even. Our proof is an easy adaption of the proof contained in [7].

Theorem 3. *Let $\nu \geq 7$ and $n = 2^\nu$. Then $\mathrm{Alt}(\mathbb{F}^\nu)$ contains an element η with $\mathrm{o}(\eta) > e^{\sqrt{(1/4)n \ln n)}}$ and $\mathrm{o}(\eta)$ even.*

Proof. Let z be a prime number such that $4 + \sum_{3 \leq p \leq z} p \leq n$, where the sum runs over distinct prime numbers from 3 to z. Then $\mathrm{Alt}(\mathbb{F}^\nu)$ contains an element η_z whose non-trivial cycles are two transpositions and some cycles with length $3, \ldots, z$. Hence $\mathrm{o}(\eta_z) = 2 \prod_{3 \leq p \leq z} p$.
If we show that there is a prime number z such that

$$4 + \sum_{3 \leq p \leq z} p \leq n \quad \text{and} \quad \ln(\mathrm{o}(\eta_z))^2 > \frac{1}{4} n \ln(n),$$

we have done.
Let $\theta(z) = \ln(\mathrm{o}(\eta_z)) = \ln(2) + \sum_{3 \leq p \leq z} \ln(p)$ and let us denote $\theta^*(z) = \theta(z) - \ln(2) = \sum_{3 \leq p < z} \ln(p)$.
Let $f(z) = \frac{z}{\ln(z)}$. Since $f(z)$ is an increasing function for real $z > e$, in the case when z is a real number and $z \geq 19$ (for $z = 19$ note that $4 + \sum_{2 < p \leq 19} p = 79 < 128 = 2^7 \leq n$), we have that

$$f(4)\ln(4) + f(3)\ln(3) = 7 < f(19)\ln(3) \leq f(z)\ln(3).$$

So, if $z \geq 19$ and $z \in \mathbb{R}$, we can write

$$\begin{aligned}
4 + \sum_{2 < p \leq z} p &= f(4)\ln(4) + \sum_{2 < p \leq z} f(p)\ln(p) \\
&= f(4)\ln(4) + f(3)\ln(3) + \sum_{3 < p \leq z} f(p)\ln(p) \\
&< f(z)\ln(3) + \sum_{3 < p \leq z} f(z)\ln(p) \\
&= \sum_{2 < p \leq z} f(z)\ln(p) = f(z) \sum_{2 < p \leq z} \ln(p) = f(z)\theta^*(z).
\end{aligned}$$

We shall choose $\bar{z} \geq 19$ such that $f(\bar{z})\theta^*(\bar{z}) = n$. Such a $\bar{z}$ exists because $f(19)\theta^*(19) < 100 < n$ and $f(z)\theta^*(z)$ is an increasing function assuming all values.
Since $\theta^*(\bar{z}) > \bar{z}/2$ for $\bar{z} \geq 19$, we have

$$n = f(\bar{z})\theta^*(\bar{z}) = \frac{\bar{z}\theta^*(\bar{z})}{\ln(\bar{z})} < \frac{2(\theta^*(\bar{z}))^2}{\ln(2\theta^*(\bar{z}))} = \frac{4(\theta^*(\bar{z}))^2}{2\ln(2\theta^*(\bar{z}))} = f(4(\theta^*(\bar{z}))^2).$$

However we also have $f(n\ln(n)) < n$. Since f is an increasing function, this shows that $n\ln(n) < 4(\theta^*(\bar{z}))^2 < 4(\theta(\bar{z}))^2$. It is now enough to consider $\tilde{z}$ as the largest prime smaller than $\bar{z}$. □

Now, we compare the estimates from Theorem 1 and Theorem 2. Take $n = 2^{128}$ and $\eta \in \mathrm{Alt}(\mathbb{F}^{128})$ such that $\mathrm{o}(\eta) \geq e^t$ ($\mathrm{o}(\eta)$ even), where $t = \sqrt{(1/4)n\ln(n)} = \sqrt{(1/4)2^{128}\ln(2^{128})}$. Since

$$e^t = e^{\sqrt{2^{126}128\ln(2)}} = e^{\sqrt{2^{133}\ln(2)}} = (e^{\sqrt{2\ln(2)}})^{2^{66}},$$

by replacing e with $2^{\log_2(e)}$, we obtain

$$e^t = (2^{\log_2(e)\sqrt{2\ln(2)}})^{2^{66}} = 2^{2^{66}\log_2(e)\sqrt{2\ln(2)}} = 2^{2^{66}\epsilon},$$

where $\epsilon \in \mathbb{R}$ is about 1.7. According to Theorem 3, $\mathrm{o}(\eta) \geq e^{2^{66}\epsilon}$. If $\mathrm{Alt}(\mathbb{F}^{128}) \subset \mathrm{GL}(\mathbb{F}^N)$, we then need the the smallest N such that $\mathrm{o}(\eta) \leq (2^{N-1} - 2)$ (Theorem 1). In other words we have to see when the following inequality holds

$$\mathrm{o}(\eta) = e^{2^{66}\epsilon} \leq (2^{N-1} - 2). \tag{6}$$

We observe that

- if $N = 2^{66}$, then (6) is false, since $2^{2^{66}\epsilon} > 2^{2^{66}} > 2^{2^{66}-1} - 2$;
- if $N = 2^{67}$, then (6) is true, since $2^{2^{66}\epsilon} < 2^{2^{66}(1.7)} < 2^{2^{67}-1} - 2$.

Therefore, we need at least $m \geq 67$ to embed $\mathrm{Alt}(\mathbb{F}^{128}) \subset \mathrm{GL}(\mathbb{F}^{2^m})$, which is exactly the same value as in Proposition 2.

5 Conclusion

In this note we provided two elementary proofs, lacking a deep algebraic background, that the round functions of the AES cipher cannot be embedded into a linear group acting on a vector space W, unless the dimension of W is at least 2^{67}. Since computing a $2^{67} \times 2^{67}$ matrix is infeasible in practice, our result shows that this attack cannot be mounted in practice. Moreover, since we do not use the specific structure of the AES in our proof of Proposition 2, we note that such result could be used also for any other block cipher $\mathcal{C}$ acting on 128−bit messages such that the group generated by its round functions is $\mathrm{Alt}(\mathbb{F}^{128})$, e.g. SERPENT [15], or $\mathrm{Sym}(\mathbb{F}^{128})$.
Moreover we observe that for any block cipher $\mathcal{C}$ acting on 64−bit messages such that $\Gamma_\infty(\mathcal{C}) = \mathrm{Alt}(\mathbb{F}^{64})$ (e.g. KASUMI [13] and a special extension of GOST [3]) with a similar argument of Lemma 1 we obtain

$$(2^6)^{11} < 2^{64}! < (2^6)^{13}.$$

Hence

$$|\mathrm{Alt}(\mathbb{F}^{64})| = \frac{|\mathrm{Sym}(2^{64})|}{2} > \frac{2^{2^{66}}}{2} = 2^{2^{66}-1} > 2^{2^{64}} = 2^{(2^{32})^2} > |\mathrm{GL}(\mathbb{F}^{2^{32}})|$$

and so if $\mathrm{Alt}(\mathbb{F}^{64}) < \mathrm{GL}(\mathbb{F}^{2^m})$, then $m \geq 33$. Also in this case, we can conclude that the embedding of GOST and KASUMI in a linear cipher is infeasible in practice.

Finally we note that the infeasibility of this type of linearization of a block cipher provides an additional motivation to check the size of the group generated by the round functions of a block cipher. In particular, it is important to check the optimal case when this group is the alternating or the symmetric group.

Acknowledgment

The authors would like to thank Rüdiger Sparr and Ralph Wernsdorf for their helpful suggestions and interesting comments.

References

[1] F. Aldà, R. Aragona, L. Nicolodi, and M. Sala. Implementation and Improvement of the Partial Sum Attack on 6-Round AES. In *Physical and Data-Link Security Techniques for Future Communication Systems*, volume 358 of *LNEE*, pages 181–195. Springer, 2015.

[2] R. Aragona, A. Caranti, F. Dalla Volta, and M. Sala. On the group generated by the round functions of translation based ciphers over arbitrary finite fields. *Finite Fields and Their Applications*, 25:293–305, 2014.

[3] R. Aragona, A. Caranti, and M. Sala. The group generated by the round functions of a GOST-like cipher. *Annali di Matematica Pura e Applicata, Online First*, pages 1–17, 2016.

[4] A. Bogdanov, D. Khovratovich, and C. Rechberger. Biclique cryptanalysis of the full AES. In *Advances in Cryptology–ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 344–371. Springer, 2011.

[5] A. Caranti, F. Dalla Volta, and M. Sala. An application of the O'Nan-Scott theorem to the group generated by the round functions of an aes-like cipher. *Designs, Codes and Cryptography*, 52(3):293–301, 2009.

[6] M. R. Darafsheh. The maximum element order in the groups related to the linear groups which is a multiple of the defining characteristic. *Finite Fields and Their Applications*, 14(4):992–1001, 2008.

[7] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163. Springer Science & Business Media, 1996.

[8] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting. Improved cryptanalysis of rijndael. In *Fast Software Encryption*, volume 1978 of *LNCS*, pages 213–230. Springer, 2001.

[9] National Bureau of Standards. The Data Encryption Standard. Federal Information Processing Standards Publication (FIPS) 46, 1977.

[10] National Institute of Standards and Technology. The Advanced Encryption Standard. Federal Information Processing Standards Publication (FIPS) 197, 2001.

[11] A. Rimoldi. On algebraic and statistical properties of AES-like ciphers. PhD thesis, University of Trento, Department of Mathematics, 2005. `http://eprints-phd.biblio.unitn.it/151/1/Provatemplate.pdf`.

[12] R. Sparr and R. Wernsdorf. Group theoretic properties of Rijndael-like ciphers. *Discrete Appl. Math.*, 156(16):3139–3149, 2008.

[13] R. Sparr and R. Wernsdorf. The round functions of KASUMI generate the alternating group. *Journal of Mathematical Cryptology*, 9(1):23–32, 2015.

[14] A. Wagner. The faithful linear representation of least degree of S_n and A_n over a field of characteristic 2. *Mathematische Zeitschrift*, 151(2):127–137, 1976.

[15] R. Wernsdorf. The round functions of SERPENT generate the alternating group. *preprint*, 2000. `http://csrc.nist.gov/archive/aes/round2/comments/20000512-rwernsdorf.pdf`.