ON THE GROUP GENERATED BY THE ROUND FUNCTIONS OF
TRANSLATION BASED CIPHERS OVER ARBITRARY FINITE FIELDS

R. ARAGONA, A. CARANTI, F. DALLA VOLTA, AND M. SALA

ABSTRACT. We define a translation based cipher over an arbitrary finite field, and study
the permutation group generated by the round functions of such a cipher. We show that un-
der certain cryptographic assumptions this group is primitive. Moreover, a minor strength-
ening of our assumptions allows us to prove that such a group is the symmetric or the
alternating group; this improves upon a previous result for the case of characteristic two.

1. INTRODUCTION

Translation based ciphers, as defined by Caranti, Dalla Volta and Sala in [CDS09], form
a class of iterated block ciphers, i.e. obtained by the composition of several key-dependent
permutations of the message/cipher space called “round functions”. This class of ciphers
contains well-known ciphers like AES [DR98] and SERPENT [ABK98].

In 1975 Coppersmith and Grossman [CG75] investigated the permutation group gener-
ated by the round functions of a cipher, aiming at finding properties of the group which
imply weaknesses of the cipher. In this direction, Kaliski et al. [KRS88] proved that if
this group is too small, then the cipher is vulnerable to certain cryptanalytic attacks. Pat-
erson [Pat99] showed that if this group is imprimitive, then it is possible to embed a trapdoor
in the cipher.

In [CDS09] the authors provided conditions on the S-Boxes of a translation based ci-
pher which ensure that the group generated by its round functions is primitive. Moreover
in [CDVS09], using the O’Nan-Scott classification of primitive groups, it was proved that
if such a cipher satisfies some additional cryptographic assumptions, then the group is the
alternating or the symmetric group.
In this paper we extend the results of [CDS09] and [CDVS09] to translation based ciphers defined over an arbitrary finite field. The main point is the move from vector spaces defined over the field \( \mathbb{F}_2 \) with two elements, to vector spaces defined over a field \( \mathbb{F}_p \), where \( p \) is an arbitrary prime. The extension to vector spaces \( V \) over an arbitrary finite field \( \mathbb{F}_q \), where \( q \) is a power of the prime \( p \), is then quite straightforward, but requires to consider \( V \) also as a vector space over the prime field \( \mathbb{F}_p \). The latter structure is completely determined by the structure of \( (V, +, 0) \) as an (elementary) abelian group. Therefore, when we will be speaking of a subspace of \( V \), we will mean an \( \mathbb{F}_q \)-subspace, while we will use the term subgroup to refer to an \( \mathbb{F}_p \)-subspace. The related terminology is explained in detail in Section 2. Readers wishing to take a quick look at the paper are advised to think of the particular case \( q = p \) throughout.

Block ciphers using algebraic structures other than the field with two elements have already been studied. For example, Biham and Shamir in [BS93] studied the security of DES against a differential attack when some of the operations in DES are replaced by addition modulo \( 2^n \). In [PRS03] Patel, Ramzan and Sundaram showed that Luby-Rackoff Ciphers are secure against adaptive chosen plaintext and ciphertext attacks, and have better time/space complexity if considered over the prime field \( \mathbb{F}_p \) for \( p > 2 \). Some result in this direction are also contained in [BBC+12].

This paper is organised as follows. After some preliminaries in Section 2, we introduce translation based ciphers over arbitrary finite fields in Section 3. In Section 4 we prove first a result (Theorem 4.4) about the primitivity of the group \( G \) generated by the round functions of a translation based cipher over an arbitrary finite field. In our main result (Theorem 4.5) we then show that this group \( G \) is actually the alternating or the symmetric group. To prove this, we follow the scheme arising from the O’Nan-Scott classification of primitive groups, in a special case dealt with by Li (Theorem 4.6), showing that all the possibilities except the alternating or symmetric group can be ruled out (Sections 5–7).

2. Preliminaries

Let \( G \) be a finite group acting transitively on a set \( V \). We will write the action of \( g \in G \) on an element \( v \in V \) as \( vg \).

A partition \( \mathcal{B} \) of \( V \) is said to be \( G \)-invariant if \( Bg \in \mathcal{B} \), for every \( B \in \mathcal{B} \) and \( g \in G \). A partition \( \mathcal{B} \) is trivial if \( \mathcal{B} = \{V\} \) or \( \mathcal{B} = \{\{v\} \mid v \in V\} \). A non-trivial \( G \)-invariant partition \( \mathcal{B} \) of \( V \) is called a block system for the action of \( G \) on \( V \). Each \( B \in \mathcal{B} \) is called a block of imprimitivity. (A block of imprimitivity can be characterised as a subset \( B \) of \( V \), which is not a singleton or the whole of \( V \), such that for all \( g \in G \) either \( B = Bg \), or \( B \cap Bg = \emptyset \).) We will say that \( G \) is imprimitive in its action on \( V \) if it admits a block system. A useful elementary fact is

**Lemma 2.1.** A block of imprimitivity is of the form \( vH \), for some \( v \in V \), where \( H \) is a proper subgroup of \( G \) properly containing the stabiliser of \( v \) in \( G \).
If $G$ is not imprimitive, then $G$ is called primitive.

In the rest of the paper $p$ is a prime, $q = p^f$ is a power of $p$, and $V$ is a vector space of dimension $d$ over the finite field $\mathbb{F}_q$.

We will be regarding $V$ also as a vector space over the prime field $\mathbb{F}_p$ of dimension $e = df$. Since the latter structure is completely determined by the (elementary) abelian group structure $(V, +, 0)$, we will refer to $\mathbb{F}_p$-subspaces of $V$ as subgroups, and we will reserve the term subspace for $\mathbb{F}_q$-subspaces of $V$. Similarly, a function on $V$ is linear if it is $\mathbb{F}_q$-linear, and additive if it is $\mathbb{F}_p$-linear.

We denote by GL$(V)$ the group of linear permutations of $V$, and by GL$(V, +, 0)$ (or simply GL$(V, +)$) the group of additive permutations of $V$. We denote by AGL$(e, p)$ the group of affine transformations of a vector space of dimension $e$ over $\mathbb{F}_p$. This is used in Section 4 and in Section 6 where some more related notation is introduced.

We write Sym$(V)$ and Alt$(V)$ respectively for the symmetric and the alternating group on the set $V$. For $v \in V$, we write $\sigma_v \in \text{Sym}(V)$ for the translation $x \mapsto x + v$ on $V$, and denote by $T(V) = \{ \sigma_v \mid v \in V \}$ the group of translations on $V$. Clearly $T(V)$ is a transitive subgroup of Sym$(V)$. Because of Lemma 2.1, $T(V)$ is always imprimitive unless $f = 1$ (that is, $q = p$ is prime) and $d = 1$.

**Lemma 2.2.** If $f > 1$, or $d > 1$, a block system for $T(V)$ is of the form $\{ W + v \mid v \in V \}$, for some proper, non-zero subgroup $W$ of $V$.

We recall that a group $G$ of permutations acting on a set $V$ is called regular if, given $v \in V$, for each $w \in V$ there exists a unique $g \in G$ such that $vg = w$ (in particular, regularity implies transitivity). The group $T(V)$ of translations is regular.

### 3. Translation Based Block Ciphers over $\mathbb{F}_q$

We consider block ciphers defined over an arbitrary finite field $\mathbb{F}_q$.

Let $\mathcal{C}$ be a block cipher for which that the plaintext space $V = (\mathbb{F}_q)^d$, for some $d \in \mathbb{N}$, coincides with the ciphertext space. According to Shannon [Sha49],

$$\mathcal{C} = \{ \tau_k \mid k \in \mathcal{K} \}$$

is a set of permutations $\tau_k$ of $V$; here $\mathcal{K}$ is the key space.

It would be very interesting to determine the group $\Gamma(\mathcal{C}) = \langle \tau_k \mid k \in \mathcal{K} \rangle \leq \text{Sym}(V)$ generated by the permutations $\tau_k$. Unfortunately, for many classical cases (e.g. AES [DR98], SERPENT [ABK98], DES [Nat77], IDEA [LM06]) this appears to be a difficult problem. However, more manageable overgroups of $\Gamma$ have been investigated (see [Wer93] [HSW94] [Wer02] [SW08]), such as the ones that we now define.

Suppose that each element of the cipher $\mathcal{C}$ is the composition of $l$ round functions, that is, permutations $\tau_{k,1}, \ldots, \tau_{k,l}$, where each $\tau_{k,h}$ is determined by a master key $k \in \mathcal{K}$, and the round index $h$. Define the groups

$$\Gamma_h(\mathcal{C}) = \langle \tau_{k,h} \mid k \in \mathcal{K} \rangle \leq \text{Sym}(V),$$
for each \( h \), and the group
\[
\Gamma_\infty(\mathcal{E}) = \langle \Gamma_h(\mathcal{E}) \mid h = 1, \ldots, l \rangle = \langle \tau_{k,h} \mid k \in \mathcal{K}, h = 1, \ldots, l \rangle
\]
In the literature, “round” often refers either to the “round index” or to the “round function”.

Consider a direct sum decomposition of \( V \)
\[
V = V_1 \oplus \cdots \oplus V_n
\]
where \( n > 1 \), and the \( V_i \) are subspaces of \( V \) with \( \dim_{\mathbb{F}_q}(V_i) = m > 1 \), for each \( i \in \{1, \ldots, n\} \), so that \( d = mn \). Each \( v \in V \) can then be written uniquely as \( v = v_1 + \cdots + v_n \), with \( v_i \in V_i \).

**Definition 3.1.** An element \( \gamma \in \text{Sym}(V) \) is called a bricklayer transformation with respect to \( (1) \) if \( \gamma \) acts on an element \( v = v_1 + \cdots + v_n \), with \( v_i \in V_i \), as
\[
v \gamma = v_1 \gamma_1 + \cdots + v_n \gamma_n,
\]
for some \( \gamma_i \in \text{Sym}(V_i) \). Each \( \gamma_i \) is called a brick.

**Definition 3.2.** A linear map \( \lambda \in \text{GL}(V) \) is called a proper mixing layer if no sum of the \( V_i \), except \( \{0\} \) and \( V \), is \( \lambda \)-invariant.

Now we generalise the definition of translation based cipher \( \mathcal{C} \) (Definition 3.1 in [CDS09], when \( \mathcal{C} \) is a block cipher over \( \mathbb{F}_q \).

**Definition 3.3.** A block cipher \( \mathcal{C} = \{ \tau_k \mid k \in \mathcal{K} \} \) over \( \mathbb{F}_q \) is called translation based (tb) if

1. each \( \tau_k \) is the composition of \( l \) round functions \( \tau_{k,h} \), for \( k \in \mathcal{K} \), and \( h = 1, \ldots, l \), where in turn each round function \( \tau_{k,h} \) can be written as a composition \( \gamma_h \lambda_h \sigma_{\phi(k,h)} \) of three permutations of \( V \), where
   - \( \gamma_h \) is a bricklayer transformation not depending on \( k \) and \( 0 \gamma_h = 0 \),
   - \( \lambda_h \) is a linear permutation not depending on \( k \),
   - \( \phi : \mathcal{K} \times \{1, \ldots, l\} \rightarrow V \) is the key scheduling function, so that \( \phi(k,h) \) is the \( h \)-th round key, given the master key \( k \);
2. for at least one round index \( h_0 \) we have that
   - \( \lambda_{h_0} \) is a proper mixing layer, and
   - the map \( \mathcal{K} \rightarrow V \) given by \( k \mapsto \phi(k,h_0) \) is surjective, that is, every element of \( V \) occurs as an \( h_0 \)-th round key.

We will refer to a round that satisfies condition (2) as a proper round.

We now work in the group \( \Gamma_h(\mathcal{E}) \), for a fixed \( h \), omitting for simplicity the indices \( h \) for the various functions. Write \( \rho = \gamma \lambda \). Note the following

**Lemma 3.4.** Suppose that for a certain \( h \), the map \( \mathcal{K} \rightarrow V \) given by \( k \mapsto \phi(k,h) \) is surjective. Then
\[
\Gamma_h(\mathcal{E}) = \langle \rho, T(V) \rangle.
\]
Proof. By assumption, $\Gamma_h(\mathcal{C}) = \langle \rho \sigma_r : r \in V \rangle$. Thus $\rho = \rho \sigma_0 \in \Gamma_h(\mathcal{C})$, so that all $\sigma_r \in \Gamma_h(\mathcal{C})$, and the statement is clear. □

**Lemma 3.5.** Suppose that for a certain $h$, the map $\mathcal{K} \to V$ given by $k \mapsto \varphi(k, h)$ is surjective.

Then if $\Gamma_h(\mathcal{C})$ is imprimitive on $V$, a block system $\mathcal{B}$ is of the form $\{W + v \mid v \in V\}$, for some proper, non-trivial subgroup $W$ of $V$.

Proof. By Lemma 3.4, $\Gamma_h(\mathcal{C})$ contains the group $T(V)$ of translations. If $\Gamma_h(\mathcal{C})$ acts imprimitively on $V$, so does $T(V)$, By Lemma 2.1, the block containing $v \in V$ is of the form $W + v$, for $W$ a proper, non-trivial subgroup of $T(V)$. □

**Proposition 3.6.** Suppose that for a certain $h$, the map $\mathcal{K} \to V$ given by $k \mapsto \varphi(k, h)$ is surjective.

Then $\Gamma_h(\mathcal{C})$ is imprimitive if and only if there exists a proper, non-trivial subgroup $W$ of $V$ such that for all $v \in V$ and $u \in W$, we have

$$(u + v)\gamma - v\gamma \in W\lambda^{-1}.$$ 

Proof. $\Gamma_h(\mathcal{C})$ is imprimitive if and only if there is a block system of type $\{W + v \mid v \in V\}$, for some proper, non-trivial subgroup $W$. Thus we have

$$(W + v)\rho = W + v\gamma \lambda \sigma_0 \implies (W + v)\gamma \lambda = W + v\gamma \lambda,$$

for every $v \in V$. Hence, for all $u \in W$ and $v \in V$ we have

$$(u + v)\gamma \lambda - v\gamma \lambda \in W,$$

so that

$$(u + v)\gamma - v\gamma \in W\lambda^{-1}.$$ 

□

4. Primitivity

We generalise the definition of weak uniformity and strong anti-invariance, given for vectorial Boolean functions in [CDS09], to any function $f : A \to A$, where $A$ is a vector space of dimension $m$ over a prime field $\mathbb{F}_p$, that is an elementary abelian group of order $p^m$.

Let $a \in A$. For every $f : A \to A$, we denote by $\hat{f}_a$ the function

$$\hat{f}_a : A \to A \quad x \mapsto f(x + a) - f(x).$$

Let $\text{Im}(\hat{f}_a) = \{y \in A \mid y = \hat{f}_a(x) \text{ for some } x \in A\}$ be the image of $\hat{f}_a$. 
Definition 4.1. For \( m \geq 2 \) and \( \delta \geq p \), let \( A \) be a subgroup of \( V \) of order \( p^m \), and \( f \in \text{Sym}(A) \). We say that \( f \) is weakly \( \delta \)-uniform if for every \( a \in A \setminus \{0\} \) we have

\[
|\text{Im}(\hat{f}_a)| > \frac{p^m - 1}{\delta}.
\]

Recently, weakly 2-uniform functions for 4 bits have been studied and classified in [FPRS12].

Remark 4.2. If a function \( f \) is weakly \( \delta \)-uniform, with \( \delta \leq p^r \) for some \( r \in \mathbb{N} \), and \( \text{Im}(\hat{f}_a) \) is contained in a subgroup \( W \) of \( A \), then

\[
|W| \geq p^m - r.
\]

Definition 4.3. Let \( A \) be a subgroup of \( V \). We say that \( f \in \text{Sym}(A) \) is strongly \( r \)-anti-invariant if for any two subgroups \( U \) and \( W \) such that \( f(U) = W \), we have either \( |U| = |W| < p^m - r \) or \( U = W = A \).

We prove the main result of this section

Theorem 4.4. Let \( C \) be a tb cipher over \( \mathbb{F}_q \).

Suppose that the \( h \)-th round is proper, and let \( 1 \leq r < \frac{m}{2} \).

If each brick of \( \gamma_h \) is

1. weakly \( p^r \)-uniform, and
2. strongly \( r \)-anti-invariant,

then \( \Gamma_h(C) \) is primitive and so also \( \Gamma_\infty(C) \) is primitive.

Proof. For the sake of simplicity we drop the round indices.

We suppose, by way of contradiction, that \( \Gamma_h(C) \) is imprimitive. By Lemma 3.5 the blocks of imprimitivity are the cosets of a subgroup of \( V \). Let \( U \) be a proper, non-trivial subgroup of \( V \) such that \( \{U + v \mid v \in V\} \) is a block system for \( G \). Since \( \gamma_0 \sigma_0 = \gamma_0 \in \Gamma_h(C) \), we have \( U \gamma_0 = U + v \), for some \( v \in V \). But \( 0 \gamma_0 = 0 \in U + v \), so

\[
(2) \quad U \gamma_0 = U.
\]

Let \( \pi_i : V \to V_i \) such that \( \pi_i(v) = v_i \) and let \( I \) be the set of all \( i \) such that \( \pi_i(U) \neq 0 \).

If \( U \cap V_i = V_i \) for every \( i \in I \), then \( U = \bigoplus_{i \in I} V_i \) and so, by definition of \( \gamma \), \( \gamma \gamma_0 = \gamma_0 \).

Hence, by (2), \( U \gamma = U \), contradicting the assumption that \( \gamma \) is a proper mixing layer.

Therefore we can suppose that there exists \( i \in I \) such that \( U \cap V_i \neq V_i \). We write \( W = U \gamma = U \gamma^{-1} \). Since \( \Gamma_h(C) \) is imprimitive, by Proposition 3.6 we have

\[
(3) \quad \hat{\gamma}_u(v) \in W
\]

for every \( u \in U \) and \( v \in V \).

Moreover, we note that

\[
(4) \quad (U \cap V_i) \gamma_i = W \cap V_i.
\]

We denote \( \gamma_i \) with \( \gamma' \). By (3) we have that \( \text{Im}(\hat{\gamma}') \subseteq W \cap V_i \) for all \( u \in U \cap V_i \). By hypothesis \( \gamma' \) is weakly \( p^r \)-uniform, so, by Remark 4.2, \( |W \cap V_i| = |U \cap V_i| \geq p^m - r \). But, by (4), this contradicts the assumption that \( \gamma' \) is strongly \( r \)-anti-invariant.

□
We are now able to state our main result.

**Theorem 4.5.** Let \( d = mn \), with \( m, n > 1 \). Let \( C \) be a tb cipher such that

1. \( C \) satisfies the hypothesis of Theorem 4.4 and
2. for all \( 0 \neq a \in V_i \), \( \{ (x + a)\gamma_i - x\gamma_i : x \in V_i \} \) is not a coset of a subgroup of \( V_i \).

Then the group \( G = \Gamma_\infty(C) \) is either \( \text{Alt}(V) \) or \( \text{Sym}(V) \).

In \([CDS09]\) it is shown that the hypothesis of Theorem 4.5 are satisfied by well-known ciphers like AES and SERPENT.

We know from Theorem 4.4 that the subgroup \( G \) of \( \text{Sym}(V) \) is primitive. We are thus able to apply the O’Nan-Scott classification of primitive groups. Actually, by Lemma 3.4, \( G \) contains the group \( T(V) \) of translations, which acts regularly on \( V \). We are then able to appeal to a result of Li \([Li03, \text{Theorem 1.1}]\) for primitive groups containing an abelian regular subgroup. In the particular case when the degree of \( G \) is a power of a prime, this states the following.

**Theorem 4.6** \([Li03, \text{Theorem 1.1}]\). Let \( G \) be a primitive group of degree \( p^b \), with \( b > 1 \).

Suppose \( G \) contains a regular abelian subgroup \( T \).

Then \( G \) is one of the following.

1. Affine, \( G \leq AGL(e, p) \), for some prime \( p \) and \( e \geq 1 \).
2. Wreath product, that is \( G \cong (S_1 \times \cdots \times S_t).O.P \), with \( p^b = c^t \) for some \( c \) and \( t > 1 \). Here \( T = T_1 \times \cdots \times T_t \), with \( T_i \leq S_i \) and \( |T_i| = c \) for each \( i \), \( S_i \cong \cdots \cong S_t \), \( O \leq \text{Out}(S_1) \times \cdots \times \text{Out}(S_t) \), \( P \) permutes transitively the \( S_i \), and one of the following holds:
   i. \( S_i, T_i = (\text{PSL}_2(11), \mathbb{Z}_{11}) \), \( S_i, T_i = (\text{M}_{11}, \mathbb{Z}_{11}) \), \( S_i, T_i = (\text{M}_{23}, \mathbb{Z}_{23}) \);
   ii. \( S_i = \text{Sym}(c) \) or \( \text{Alt}(c) \), and \( T_i \) is an abelian group of order \( c \).
3. Almost simple, that is, \( S \leq G \leq \text{Aut}(S) \), for a nonabelian simple group \( S \).

Here the notation \( S.T \) denotes an extension of the group \( S \) by the group \( T \).

In the next three Sections we will examine the three cases of Theorem 4.6 and show that the only possibilities for our \( G \) is to be the full alternating or symmetric group. (Note that these two groups fall under the almost simple case.) This will prove Theorem 4.5.

### 5. The Almost Simple Case

In the almost simple case (3), we note that \( S \) is a transitive subgroup of the primitive group \( G \), so the intersection of a one-point stabiliser in \( G \) with \( S \) is a proper subgroup of \( S \) of index \( p^b \), where \( b = \text{fnn} \) with \( m, n > 1 \), i.e. \( b > 3 \). By Theorem 1 and Section (3.3) in \([Gur83]\), the only nonabelian simple groups that have a subgroup of index \( p^b \) with \( b > 3 \), are the alternating group and the group \( \text{PSL}_\alpha(\beta) \), where
(i) \((\beta^a - 1)/(\beta - 1) = p^b\),
(ii) \(\alpha\) is a prime, and
(iii) \(\beta\) is a power of a prime \(\pi\) such that \(\pi \equiv 1 \mod \alpha\).

If \(S = \text{Alt}( \varphi )\), since \(\text{Aut}( \text{Alt}( \varphi )) = \text{Sym}( \varphi )\), then \(G\) is either \(\text{Alt}( \varphi )\) or \(\text{Sym}( \varphi )\).

In our case, we can rule out \(S = \text{PSL}_\alpha(\beta)\) as follows. First we note that by (iii), we have \(\beta^i \equiv 1 \mod \alpha\), for each \(i\). So
\[
(\beta^a - 1)/(\beta - 1) = \beta^{a-1} + \beta^{a-2} + \cdots + \beta + 1 \equiv \alpha \mod \alpha,
\]
i.e., \(\alpha\) divides \(\beta^{a-1} + \beta^{a-2} + \cdots + \beta + 1\), and then, by (i) we have that \(\alpha\) divides \(p^b\).
Hence \(\alpha = p\), since \(\alpha\) is a prime. By (iii) we have \(\beta = kp + 1\) for some \(k \in 2\mathbb{N}\), therefore
\[
\beta^{p-1} + \beta^{p-2} + \cdots + \beta + 1 = (kp + 1)^{p-1} + (kp + 1)^{p-2} + \cdots + (kp + 1) + 1 = p^b.
\]

So we have
\[
(\sum_{j=1}^{p-1} \sum_{i=1}^{p-1-j} \binom{p-j}{i} k^i p^j) + p = p^b.
\]
Dividing (5) by \(p\), we obtain
\[
(\sum_{j=1}^{p-1} \sum_{i=1}^{p-1-j} \binom{p-j}{i} k^i p^{j-1}) + 1 = p^{b-1}.
\]
Rewrite (6) as follows
\[
(\sum_{j=1}^{p-1} \sum_{i=2}^{p-1} \binom{p-j}{i} k^i p^{j-1}) + \left(\sum_{j=1}^{p-1} \binom{p-j}{1} k\right) = p^{b-1} - 1.
\]
Since
\[
\sum_{j=1}^{p-1} (p-j)k = \sum_{j=1}^{p-1} (p-j)k = \sum_{j=1}^{p-1} jk = \frac{(p-1)pk}{2},
\]
then the left side of (7) is divisible by \(p\) and the right side of (7) is not divisible by \(p\). So we conclude that \((\beta^{p-1} - 1)/(\beta - 1) = p^b\), is not possible if \(b > 1\), which is our hypothesis.

6. The Affine Case

As observed by Li [Li03], if \(V = (V, +, 0)\) is a vector space over the field \(\mathbb{F}_p\), the symmetric group \(\text{Sym}(V)\) will contain in general many isomorphic copies of the affine group. The obvious one, \(\text{AGL}(V, +, 0)\), consists of the maps \(x \mapsto xg + v\), where \(g \in \text{GL}(V, +, 0)\), and \(v \in V\). But there are in general several structures \((V, \circ, \Theta)\) of an \(\mathbb{F}_p\)-vector space on the set \(V\) (where \(\Theta\) is the neutral element for \(\circ\)), each of which will yield in general a different copy \(\text{AGL}(V, \circ, \Theta)\) of the affine group within \(\text{Sym}(V)\), consisting of the maps \(x \mapsto xg + v\), where \(g \in \text{GL}(V, \circ, \Theta)\), and \(v \in V\).
In this section, we assume that the group $G = \Gamma_\infty(\mathcal{G})$ generated by the round functions is contained in the affine subgroup $AGL(V, \circ, \Theta)$ with respect to the elementary abelian group (i.e., $\mathbb{F}_p$-vector space) structure $(V, \circ, \Theta)$. Since by our assumptions the group $T = T(V)$ of translations with respect to $+$ is contained in $G$, we obtain that $T$ is an abelian regular subgroup of $AGL(V, \circ, \Theta)$. This allows us to use the description of [CDVS06] for this kind of subgroups, which we revisit in the following. This is an extension (and a correction) of the work of [CDS09] for characteristic 2. Although the approach of [CDVS06] in terms of rings has proved useful in other circumstances, in this particular case we believe a treatment without rings to be preferable in terms of clarity.

So we have that the translations $\sigma_y : x \mapsto x + y$ are in the affine group $AGL(V, \circ, \Theta)$. Thus for $x, y \in V$, if we consider the translation $\sigma_{y \circ \Theta}$, that takes $\Theta$ to $y$, we have

$$x + y - \Theta = x\sigma_{y \circ \Theta} = x\kappa(y) \circ y,$$

for some $\kappa(y) \in GL(V, \circ, \Theta)$. A substitution shows that

$$x \circ y = x\kappa(y)^{-1} + y - \Theta.$$

In the following we will be using (8) and (9) repeatedly without further mention.

Note that

$$x + y + z - 2\Theta = (x + y - \Theta) + (z - \Theta)$$

$$= (x\kappa(y) \circ y) + z - \Theta$$

$$= x\kappa(y)\kappa(z) \circ y\kappa(z) \circ z$$

and also

$$x + y + z - 2\Theta = x - \Theta + (y + z - \Theta)$$

$$= x - \Theta + (y\kappa(z) \circ z)$$

$$= x\kappa(y\kappa(z) \circ z) \circ y\kappa(z) \circ z$$

so that

$$\kappa(y + z - \Theta) = \kappa(y\kappa(z) \circ z) = \kappa(y)\kappa(z).$$

This shows that $\kappa(V) = \{ \kappa(y) \mid y \in V \}$ is a group, and $y \mapsto \kappa(y + \Theta)$ is an epimorphism $(V, +) \to \kappa(V)$, so that $\kappa(V)$ is a $p$-group, and thus acts unipotently on $(V, \circ)$. Note that we have $\kappa(\Theta) = I$ (set $y = z = \Theta$ in (11)), and

$$\kappa(y)^{-1} = \kappa(-y + 2\Theta)$$

(set $z = -y + 2\Theta$ in (11)).

Now fix $y \in V$, $y \neq \Theta$, such that $y\kappa(x) = y$ for all $x \in V$. (Since the group $\kappa(V)$ is unipotent on $(V, \circ)$, we have $\{ y \in V \mid y\kappa(x) = y \text{ for all } x \in V \} \neq \{ \Theta \}$.)

Note that $\rho$ is $\circ$-affine, so there is a constant $\eta$ such that $s \mapsto s\rho \circ \eta$ is $\circ$-additive. It follows that $(s \circ t)\rho \circ \eta = s\rho \circ \eta \circ t\rho \circ \eta$, so that

$$(s \circ t)\rho = s\rho \circ t\rho \circ \eta$$
for all \( s, t \in V \). We use this to compute, for the given \( y \) and an arbitrary \( x \in V \),

\[
(x + (y - \Theta))\rho - x\rho = (y + x - \Theta)\rho - x\rho \\
= (y\kappa(x) \circ x)\rho - x\rho \\
= (y \circ x)\rho - x\rho \\
= y\rho \circ x\rho \circ \eta - x\rho \\
= (y\rho \circ \eta) \circ x\rho - x\rho \\
= (y\rho \circ \eta)\kappa(x\rho)^{-1} + x\rho - \Theta - x\rho \\
= (y\rho \circ \eta)\kappa(x\rho)^{-1} - \Theta.
\]

Write

\[
u = y\rho \circ \eta, \quad v = -x\rho + 2\Theta,
\]

so that \( \kappa(v) = \kappa(x\rho)^{-1} \) by (12). Now (13) becomes

\[
(x + (y - \Theta))\rho - x\rho = u\kappa(v) - \Theta.
\]

Write \( \kappa(v) = 1 \circ \delta(v) \), that is,

\[
u\kappa(v) = u \circ u\delta(v)
\]

for \( u \in V \), where \( \delta : V \to \text{End}(V, \circ) \). Then, as shown in [CDVS06], \( \delta \) is \( \circ \)-additive, that is, \( \delta(v_1 \circ v_2) = \delta(v_1) \circ \delta(v_2) \) for \( v_1, v_2 \in V \). (This follows from (10), since interchanging \( y \) and \( z \), and setting \( x = \Theta \), we obtain \( y\kappa(z) \circ z = z\kappa(y) \circ y \), so that \( y\delta(z) = z\delta(y) \). Now the left-hand side of the latter equation is \( \circ \)-additive in \( y \), and thus so is the right-hand side.)

From the \( \circ \)-additivity of \( \delta \) it follows that

\[
W = u\delta(V) = \{u\delta(v) \mid v \in V\}
\]

is a \( \circ \)-subgroup of \( V \), and then

\[
\{u\kappa(v) \mid v \in V\} = \{u \circ u\delta(v) \mid v \in V\} = u \circ u\delta(V) = u \circ W
\]

is a \( \circ \)-coset of the \( \circ \)-subgroup \( W \).

We want to show next that \( W \) is invariant under \( \kappa(V) \). For \( z \in V \) we have

\[
u\delta(v)\kappa(z) = u\delta(v) \circ u\delta(v)\delta(z).
\]

The first summand \( u\delta(v) \) in the right-hand side is in \( W \); we want to prove that also \( u\delta(v)\delta(z) \) is in \( W \). Now (11) implies, for \( v, z \in V \),

\[
d(v + z - \Theta) = \delta(v) \circ \delta(z) \circ \delta(v)\delta(z),
\]

so that

\[
\delta(v)\delta(z) = \delta(v + z - \Theta) \circ (\ominus\delta(v)) \circ (\ominus\delta(z)),
\]

where \( \ominus t \) is the opposite of \( t \) with respect to \( \circ \). It follows that also \( u\delta(v)\delta(z) \in W \), so that by (16) \( u\delta(v)\kappa(z) \in W \), that is, \( W \) is \( \kappa(V) \)-invariant.
From this it follows that \( W - \Theta \) is a \(+\)-subgroup of \( V \), as
\[
(u\delta(v_1) - \Theta) + (u\delta(v_2) - \Theta) = u\delta(v_1)\kappa(u\delta(v_2)) \circ u\delta(v_2) - \Theta \in W - \Theta.
\]

Now the right-hand side of (14) reads
\[
uk(v) - \Theta = u \circ u\delta(v) - \Theta
\]
\[
= u\delta(v) \circ u - \Theta
\]
\[
= u\delta(v)\kappa(u)^{-1} + u - 2\Theta.
\]

So if we take a fixed value of \( \Theta \), as chosen above, and let \( x \) (and thus \( v \)) range in \( V \), we obtain from (14) and (17) that the set
\[
\{(x + (y - \Theta))\rho - x\rho : x \in V\} = W\kappa(u)^{-1} + u - 2\Theta = (u - \Theta) + (W - \Theta)
\]
is a \(+\)-coset with respect to \( u - \Theta \) of the \(+\)-subgroup \( W - \Theta \) of \( V \).

Now \( \lambda \) is additive with respect to \(+\), so, if we apply \( \lambda^{-1} \) to (18), we obtain that
\[
\{(x + (y - \Theta))\gamma - x\gamma : x \in V\}
\]
is also a \(+\)-coset of the \(+\)-subgroup \( W - \Theta \) of \( V \).

Now we can choose an index \( i \) such that the component \( y_i \in V_i \) of \( y \neq \Theta \) is different from \( \Theta \). This is because either \( \Theta = 0 \), and then \( y \neq 0 \) must have a non-zero component; or \( \Theta \neq 0 \), and then \( \Theta \) can only be in at most a single component \( V_{i_0} \), so in case it suffices to choose \( i \neq i_0 \). With this choice, we have that the projection
\[
\{(x + (y_i - \Theta))\gamma_i - x\gamma_i : x \in V_i\}
\]
of the set (19) on \( V_i \) is a \(+\)-coset of a subgroup of \( V_i \) with respect to \(+\) and so we obtain a contradiction to assumption (2) of Theorem 4.5.

7. The wreath product case

Let \( G = \Gamma_\infty(\mathcal{C}) \) be the wreath product in product action as follows
\[
G = (S_1 \times \cdots \times S_c).O.P
\]
with \( \rho^h = z^c \) for some \( z \) and \( c > 1 \). Here \( T = T_1 \times \cdots \times T_c \), with \( T_i \leq S_i \) and \( |T_i| = z \) for each \( i \), \( S_1 \cong \cdots \cong S_c \), \( O \leq \text{Out}(S_1) \times \cdots \times \text{Out}(S_c) \), \( P \) permutes transitively the \( S_i \)'s by conjugation. It follows that \( S_1 \times \cdots \times S_c = \text{Soc}(G) \).

By Lemma 3.3, \( G = \langle T, \rho \rangle \), and \( T \leq \text{Soc}(G) \), so that \( G/\text{Soc}(G) \) is cyclic, spanned by \( \rho \). Moreover, since \( P \) permutes transitively the \( S_i \), then \( \rho \) permutes cyclically the \( S_i \) by conjugation. So we have, possibly reordering indices, \( S_i^\rho = \rho^{-1}S_i\rho = S_{i+1} \) for each \( i \neq c \) and \( S_c^\rho = S_1 \).
Since each $T_i$ is a group of translations, then $W_i = 0T_i \subseteq S_i$ is a subgroup of $V$ of order $z$. But also $0S_i$ has order $z$, so $0T_i = 0S_i$ for each $i$. Each element $v$ of $V$ can be written uniquely as

$$v = 0t_1t_2 \cdots t_c = 0t_1 + \cdots + 0t_c$$

where $t = t_1t_2 \cdots t_c$ for each $t_i \in T_i$ and so

$$V = W_1 \oplus \cdots \oplus W_c.$$

For each $i$, $W_i\rho = 0S_i\rho = 0S_{i+1}^{-1}\rho = 0\rho S_{i+1} = 0S_{i+1} = W_{i+1}$, since $0\rho = 0$. Hence $\rho$ permutes cyclically the $W_i$. Write $v \in V$ as $v = \hat{v} + w_1 + \cdots + w_c$, with $w_i \in W_i$, and $w_i = 0t_i$ for each $t_i \in T_i$. So we have

$$v\rho = (0t_1 + \cdots + 0t_c)\rho = 0t_1 \cdots t_c\rho = 0t_1^0 \cdots t_c^0$$

as the $t_i$ are translations and $0\rho^{-1} = 0$. Since $t_i^0 \in S_i^0 = S_{i+1}$, there exist $t_{i+1}' \in T_{i+1}$ such that $0t_i^0 = 0t_i\rho = 0t_{i+1}' \in W_{i+1}$ (with indices taken modulo $c$), and because $S_i$ and $S_j$ commute elementwise, we have

$$v\rho = 0t_1^0 \cdots t_c^0 = 0t_1''t_2'' \cdots t_c'' = 0t_1^1t_2^1 \cdots t_c^1 = \cdots$$

$$= 0t_1't_2't_3' \cdots t_c' = 0t_1' + \cdots + 0t_c' = 0t_1\rho + 0t_1\rho + \cdots + 0t_c\rho = w_1\rho + \cdots + w_c\rho.$$

Now we fix an index $i$ and we take $u \in W_i$. We have

$$v\rho = (w_1 + \cdots + w_c)\rho = w_1\rho + \cdots + w_c\rho$$

where $w_i\rho \in W_{i+1}$. We also have

$$(v + u)\rho = w_1\rho + \cdots + (w_1 + u)\rho + \cdots + w_c\rho$$

with $(w_1 + u)\rho \in W_{i+1}$. It follows that

$$(v + u)\rho - v\rho = (w_1 + u)\rho - w_1\rho \in W_{i+1}.$$

We recall that $\rho = \gamma\lambda$, with $\lambda$ additive. So, applying $\lambda^{-1}$ to both sides of (20), we obtain

$$(\gamma + u)\lambda - v\lambda = \gamma + u\lambda - v\lambda \in W_{i+1}\lambda^{-1}.$$

Let $\pi_j : V \to V_j$ such that $\pi_j(v) = v_j$ and let $J$ be the set of all $j$ such that $\pi_j(W_i) \neq 0$. Now we have two cases.

(1) If $W_i \cap V_j = V_j$ for every $j \in J$, then $W_i = \bigoplus_{j \in J} V_j$, so $W_i\gamma = W_i$. Since $W_i\rho = W_{i+1}$, we have $W_i = W_i\gamma = W_{i+1}\lambda^{-1}$ and so, by (21), $(v + u)\gamma - v\gamma \in W_i$, for all $v \in V$ and $u \in W_i$. By Proposition 3.6 it follows that $G$ is imprimitive, but this contradicts Theorem 4.4.
(II) Otherwise, there exist $j$ such that $W_t \cap V_j \neq V_j$. We denote $U = W_t$ and $U' = W_{t+1}\lambda^{-1}$ and we note that

$$(U \cap V_j)\gamma'_j = U' \cap V_j.$$  

We denote $\gamma_j$ with $\gamma'$. By (21), we have that $\text{Im}(\gamma'_j) \subseteq U' \cap V_j$ for all $u \in U \cap V_j$. By assumption $\gamma'$ is weakly $p^r$-uniform, so, by Remark 4.2, $|U' \cap V_j| = |U \cap V_j| \geq p^{m-r}$. But this contradicts (22), since $\gamma'$ is strongly $r$-anti-invariant.

ACKNOWLEDGEMENTS

The authors are grateful to the referees for several useful suggestions. We are particularly indebted to one of the referees for pointing out an inconsistency in a previous version, and for suggesting the way to fix it.

REFERENCES

[ABK98] R. J. Anderson, E. Biham, and L.R. Knudsen, SERPENT: A new block cipher proposal, Fast Software Encryption, LNCS, vol. 1372, Springer, 1998, pp. 222–238.

[BBC+12] L. Babinkostova, K. W. Bombardier, M. M. Cole, T. A. Morreell, and C. B. Scott, Algebraic properties of generalized Rijndael-like ciphers, arXiv (2012), http://arxiv.org/pdf/1210.7942v4.pdf.

[BS93] E. Biham and A. Shamir, Differential cryptanalysis of the data encryption standard, Springer-Verlag, New York, 1993.

[CDS09] A. Caranti, F. Dalla Volta, and M. Sala, On some block ciphers and imprimitive groups, AAECC 20 (2009), no. 5-6, 229–350.

[CDVS06] A. Caranti, F. Dalla Volta, and M. Sala, Abelian regular subgroups of the affine group and radical rings, Publ. Math. Debrecen 69 (2006), no. 3, 297–308.

[CDVS09] ———, An application of the O’Nan-Scott theorem to the group generated by the round functions of an AES-like cipher, Des. Codes Cryptogr. 52 (2009), no. 3, 293–301.

[CG75] D. Coppersmith and E. Grossman, Generators for certain alternating groups with applications to cryptography, SIAM J. Appl. Math. 29 (1975), no. 4, 624–627.

[DR98] J. Daemen and V. Rijmen, AES proposal: Rijndael, Tech. report, NIST, 1998, http://www.nist.gov/aes.

[FPRS12] C. Fontanari, V. Pulice, A. Rimoldi, and M. Sala, On weakly apn functions and 4-bit s-boxes, Finite Fields and Their Applications 18 (2012), no. 3, 522–528.

[Gur83] R. M. Guralnick, Subgroups of prime power index in a simple group, J. Algebra 81 (1983), 304–311.

[HSW94] G. Hornauer, W. Stephan, and R. Wernsdorf, Markov ciphers and alternating groups, Advances in cryptology—EUROCRYPT ’93 (Loftus, 1993), Lecture Notes in Comput. Sci., vol. 765, Springer, Berlin, 1994, pp. 453–460. MR 1290337 (95e:94031)

[KRS88] B. S. Kaliski, Jr., R. L. Rivest, and A. T. Sherman, Is the data encryption standard a group? (Results of cycling experiments on DES), J. Cryptology 1 (1988), no. 1, 3–36.

[Li03] C. H. Li, The finite primitive permutation groups containing an abelian regular subgroup, Proc. London Math. Soc. 87 (2003), no. 3, 725–747.

[LM06] X. Lai and J. L. Massey, A proposal for a new block encryption standard, Advances in Cryptology-EUROCRYPT’90, LNCS, vol. 473, Springer, 2006, pp. 389–404.
[Nat77] National Bureau of Standards, *The Data Encryption Standard*, Federal Information Processing Standards Publication (FIPS) 46, 1977.

[Pat99] K. G. Paterson, *Imprimitive permutation groups and trapdoors in iterated block ciphers*, Fast software encryption, LNCS, vol. 1636, Springer, Berlin, 1999, pp. 201–214.

[PRS03] S. Patel, Z. Ramzan, and G. S. Sundaram, *Luby-Rackoff ciphers: Why XOR is not so exclusive*, Selected areas in cryptography, Lecture Notes in Comput. Sci., vol. 2595, Springer, Berlin, 2003, pp. 271–290.

[Sha49] C. E. Shannon, *Communication theory of secrecy systems*, Bell System Tech. J. 28 (1949), 656–715. MR 0032133 (11,258d)

[SW08] R. Sparr and R. Wernsdorf, *Group theoretic properties of Rijndael-like ciphers*, Discrete Appl. Math. 156 (2008), no. 16, 3139–3149. MR 2462120 (2010d:94114)

[Wet93] R. Wernsdorf, *The one-round functions of the DES generate the alternating group*, Advances in cryptology—EUROCRYPT ’92 (Balatonfüred, 1992), Lecture Notes in Comput. Sci., vol. 658, Springer, Berlin, 1993, pp. 99–112. MR 1243663 (94g:94031)

[Wet02] ———, *The round functions of RIJNDAEL generate the alternating group*, Proceedings of the 9th International Workshop on Fast Software Encryption, Leuven, Belgium, February 2002, Lecture Notes in Comput. Sci., vol. 2365, Springer, Heidelberg, 2002, pp. 143–148.

(Aragona) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TRENTO, VIA SOMMARIVE 14, 38123 TRENTO, ITALY

E-mail address: ric.aragona@gmail.com

(Caranti) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TRENTO, VIA SOMMARIVE 14, 38123 TRENTO, ITALY

E-mail address: andrea.caranti@unitn.it

(Dalla Volta) DEPARTMENT OF MATHEMATICS AND APPLICATIONS, UNIVERSITY OF MILANO-BICOCCA, VIA R. COZZI, 53, 20126 MILANO, ITALY

E-mail address: francesca.dallavolta@unimib.it

(Sala) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TRENTO, VIA SOMMARIVE 14, 38123 TRENTO, ITALY

E-mail address: maxsalacodes@gmail.com