On differential uniformity of maps that may hide an algebraic trapdoor

Marco Calderini and Massimiliano Sala

Department of Mathematics, University of Trento, Italy
marco.calderini@unitn.it, maxsalacodes@gmail.com

Abstract. We investigate some differential properties for permutations in the affine group, of a vector space V over the binary field, with respect to a new group operation $\circ$, inducing an alternative vector space structure on V.

1 Introduction

Most modern block ciphers are built using components whose cryptographic strength is evaluated in terms of the resistance offered to attacks on the whole cipher. For example, differential properties of Boolean functions are studied for the S-Boxes to thwart differential cryptanalysis ([3,10]).

Little is known on similar properties to avoid trapdoors in the design of the block cipher. In [6] the authors investigate the minimal properties for the S-Boxes (and the mixing layer) of an AES-like cipher (more precisely, a translation-based cipher, or tb cipher) to thwart the trapdoor coming from the imprimitivity action, first noted in [11] .

In [8], Li observed that if V is a finite vector space over a finite field $\mathbb{F}_p$, the symmetric group $\mathrm{Sym}(V)$ will contain many isomorphic copies of the affine group $\mathrm{AGL}(V)$, which are its conjugates in $\mathrm{Sym}(V)$. So there are several structures $(V, \circ)$ of a $\mathbb{F}_p$-vector space on the set V , where $(V, \circ)$ is the abelian additive group of the vector space. Each of these structure will yield in general a different copy $\mathrm{AGL}(V, \circ)$ of the affine group within $\mathrm{Sym}(V)$. So, a trapdoor coming from an alternative vector space structure, which we call *hidden sum*, can be embedded in a cipher, whenever the permutation group generated by the round functions of the cipher is contained in a conjugate of $\mathrm{AGL}(V)$. In [5] the authors provide conditions on the S-Boxes of a tb cipher that avoid attacks coming from hidden sums. This result has been generalized to tb ciphers over any field

in [2]. Also, in [1], the authors studied such trapdoors, characterizing a new class of vectorial Boolean functions, which they call *anti-crooked*, able to avoid any hidden sum.

In the yet unpublished Ph.D thesis [9] the author investigated some properties of affine groups, of a vector space over the binary field, with respect to a hidden sum $\circ$. In particular, he focused on affine groups which contain the translation group with respect to the usual sum $+$, and affine groups whom translation group is contained in AGL(V). In this paper we study the differential properties of maps which are affine w.r.t. a hidden sum. Our results are presented in Section 3, while in Section 2 we provide some preliminaries from previous works. Our main result, Theorem 3, concludes Section 3. Section 4 concludes this paper with the sketch of an actual attack to a cipher in which a hidden sum trapdoor is embedded.

2 Preliminaries

Here we give some notation and some known results that we are going to use along the paper. In the following, if not specified, V will be an n-dimensional vector space over $\mathbb{F}_2$.

With the symbol $+$ we refer to the usual sum over the vector space V, and we denote by T_+, AGL($V, +$) and GL($V, +$), respectively, the translation, affine and linear groups w.r.t. $+$.

We recall that a p-elementary group G acting on a set Ω is a group of permutations on Ω such that for all g in G we have $g^p = Id_\Omega$.
A group G is called regular if for all a and b in Ω there exists a unique g in G such that $g(a) = b$.

Remark 1. An elementary group acting on a vector space $V = \mathbb{F}_p^n$ is obviously a p-elementary group. The translation group of V is an elementary abelian regular group. Vice versa, we claim that if T is an elementary abelian regular group, there exists a vector space structure $(V, \circ)$ such that T is the related translation group. In fact, from the regularity of T we have $T = \{\tau_a \,|\, a \in V\}$ where τ_a is the unique map in T such that $0 \mapsto a$. Then, defining the sum $x \circ a := \tau_a(x)$, it is easy to check that $(V, \circ)$ is a commutative group, and so we can consider the group operation as a sum, making it an additive group without loss of generality. Moreover, let the multiplication of a vector by an element of $\mathbb{F}_p$ defined by

$$sv := \underbrace{v \circ \cdots \circ v}_{s}, \text{ for all } s \in \mathbb{F}_p,$$

then it is easy to check that for all $s, t \in \mathbb{F}_p$, and $v, w \in V$

$$s(v \circ w) = sv \circ sw,$$

$$(s + t)v = sv \circ tv,$$

$$(st)v = s(tv)$$

and being T p-elementary $pv = 0$. Thus $(V, \circ)$ is a vector space over $\mathbb{F}_p$. Observe that $(V, \circ)$ and $(V, +)$ are isomorphic vector space (since $|V| < \infty$).

For abelian regular subgroups of the affine group in [4] the authors give a description of these in terms of commutative associative algebras that one can impose on the vector space $(V, +)$ or, in other words, of products that can be defined on V and distribute the sum $+$. We report the principal result shown in [4]. Recall that a (Jacobson) radical ring is a ring $(V, +, \cdot)$ in which every element is invertible with respect to the circle operation $x \circ y = x + y + x \cdot y$, so that $(V, \circ)$ is a group. The circle operation may induce a vector space structure on V or not.

Theorem 1. *Let $\mathbb{F}$ be an arbitrary field, and $(V, +)$ a vector space of arbitrary dimension over $\mathbb{F}$.*
There is a one-to-one correspondence between

1) *abelian regular subgroups T of $\mathrm{AGL}(V, +)$, and*
2) *commutative, associative $\mathbb{F}$-algebra structures $(V, +, \cdot)$ that one can impose on the vector space structure $(V, +)$, such that the resulting ring is radical.*

In this correspondence, isomorphism classes of $\mathbb{F}$-algebras correspond to conjugacy classes under the action of $\mathrm{GL}(V, +)$ of abelian regular subgroups of $\mathrm{AGL}(V, +)$.

We recall that an exterior algebra over an $\mathbb{F}$-vector space V is the $\mathbb{F}$-algebra whose product is the wedge product $\wedge$ having the following properties:

1) $x \wedge x = 0$ for all $x \in V$,
2) $x \wedge y = -y \wedge x$.

The elements of the exterior algebra over V are linear combinations of monomials such as $u, v \wedge w, x \wedge y \wedge z$, etc., where u, v, w, x, y, and z are vectors of V.

Remark 2. From the theorem above we can note that in characteristic 2, algebras corresponding to elementary abelian regular subgroups of $\mathrm{AGL}(V, +)$ are exterior algebras or a quotient thereof.

We will denote by σ_a the translation in T_+ such that $x \mapsto x + a$. We will use $T_\circ$ and $\mathrm{AGL}(V, \circ)$ to denote the translation and affine group corresponding to a hidden sum $\circ$, that is when $(V, \circ)$ is a vector space and so $T_\circ$ is elementary abelian and regular.
As noted in the remark above, since $T_\circ$ is regular, for each $a \in V$ there is a unique map $\tau_a \in T_\circ$ such that $0 \mapsto a$. Thus

$$T_\circ = \{\tau_a \mid a \in V\}.$$

The relation between $T_\circ$ and $\mathrm{AGL}(V, \circ)$ is that $\mathrm{AGL}(V, \circ)$ is the normalizer of $T_\circ$ in $\mathrm{Sym}(V)$, that is $\mathrm{AGL}(V, \circ)$ is the largest subgroup of $\mathrm{Sym}(V)$ contaning $T_\circ$ such that $T_\circ$ is normal in it. Indeed, $\mathrm{AGL}(V, +)$ is the normalizer of T_+ and they are, respectively, the isomorphic images of $\mathrm{AGL}(V, \circ)$ and $T_\circ$. With 1_V we will denote the identity map of V.

Remark 3. If $T_\circ \subseteq \mathrm{AGL}(V, +)$, then $\tau_a = \sigma_a \kappa$ for some $\kappa \in \mathrm{GL}(V, +)$, since $\mathrm{AGL}(V, +) = \mathrm{GL}(V, +) \ltimes T_+$. We will denote by κ_a the linear map κ corresponding to τ_a.

Let $T \subseteq \mathrm{AGL}(V, +)$ and define the set

$$U(T) = \{a \mid \tau = \sigma_a, \tau \in T\}.$$

It is easy to check that $U(T)$ is a subspace of V, whenever T is a subgroup. If $T = T_\circ$ for some operation $\circ$, then $U(T_\circ)$ is not empty for the following lemma.

Lemma 1 ([4]). *Let T_+ be the group of translation in $\mathrm{AGL}(V, +)$ and let $T \subseteq \mathrm{AGL}(V, +)$ be a regular subgroup. Then, if V is finite $T_+ \cap T$ is nontrivial.*

$U(T_\circ)$ is important in the context of our theory and its dimension gives fundamental information on the corresponding hidden sum.

3   On the differential uniformity of a ∘-affine map

Any round function of a translation-based block cipher (Definition 3.1 [6]) is composed by a parallel s-Box γ, a mixing layer λ and a translation σ_k by the round key. The map γ must be as non-linear as possible to

create confusion in the message. An important notion of "non-linearity" of Boolean functions is the differential uniformity.

In this section we establish a lower bound on the differential uniformity of the maps lying in some $\mathrm{AGL}(V, \circ)$. We will consider the two cases of affine group $\mathrm{AGL}(V, \circ)$ such that $T_\circ \subseteq \mathrm{AGL}(V, +)$ and/or $T_+ \subseteq \mathrm{AGL}(V, \circ)$. In both cases in the following proofs we can consider w.l.o.g. maps f such that $f(0) = 0$. In fact in the first case we can compose f with $\tau_{f(0)}$ that maps $f(0)$ to 0 and in the second case we compose with $\sigma_{f(0)}$, in both cases we compose with an affine map.

We recall the definition of differential uniformity.

Definition 1. *Let* $m, n \geq 1$. *Let* $f : \mathbb{E}_2^m \to \mathbb{F}_2^n$, *for any* $a \in \mathbb{E}_2^m$ *and* $b \in \mathbb{F}_2^n$ *we define*

$$\delta_f(a, b) = |\{x \in \mathbb{E}_2^m \mid f(x + a) + f(x) = b\}|.$$

The differential uniformity *of f is*

$$\delta(f) = \max_{\substack{a \in \mathbb{E}_2^m, \, b \in \mathbb{E}_2^n \\ a \neq 0}} \delta_f(a, b).$$

f is said δ-differential uniform *if $\delta = \delta(f)$.*

We are ready for our first result.

Lemma 2. *Let* $T_\circ \subseteq \mathrm{AGL}(V, +)$ *and* $\dim(U(T_\circ)) = k$. *Then* $f \in \mathrm{AGL}(V, \circ)$ *is at least 2^k differentially uniform.*

Proof. Let $a \in U(T_\circ)$, then

$$f(x + a) + f(x) = f(x \circ a) + f(x) = (f(x) \circ f(a)) + f(x).$$

So, for all $f(x) \in U(T_\circ)$ we have

$$(f(x) \circ f(a)) + f(x) = (f(x) + f(a)) + f(x) = f(a),$$

that implies $|\{x \mid f(x + a) + f(x) = f(a)\}| \geq 2^k$.

When $T_+ \subseteq \mathrm{AGL}(V, \circ)$, we can define $U_\circ(T_+) = \{a \mid \sigma_a \in T_+ \cap T_\circ\}$ and it is a vector subspace of $(V, \circ)$. Then we obtain, analogously, the following lemma.

Lemma 3. *Let* $T_+ \subseteq \mathrm{AGL}(V, \circ)$ *and* $\dim(U_\circ(T_+)) = k$, *as a subspace of* $(V, \circ)$. *Then* $f \in \mathrm{AGL}(V, \circ)$ *is at least 2^k differentially uniform.*

Recalling that given a ring R, $r \in R$ is called nilpotent if there exists an integer n such that $r^n = 0$, while $r \in R$ is called unipotent if and only if $r - 1$ is nilpotent, we have the following:

Lemma 4. *Let $T_\circ \subseteq \mathrm{AGL}(V, +)$. Then for each $a \in V$, κ_a has order 2 and it is unipotent.*

Proof. We know that τ_a has order 2, because $T_\circ$ is elementary. Then, $\tau_a^2 = 1_V$ implies $\tau_a(a) = 0$, and in particular $\kappa_a(a) = a$. So

$$x = \tau_a^2(x) = \kappa_a(\kappa_a(x) + a) + a = \kappa_a^2(x) + a + a = \kappa_a^2(x) \quad \text{for all } x \in V.$$

That implies $(\kappa_a - 1_V)^2 = \kappa_a^2 - 1_V = 0$. $\qquad\blacksquare$

Remark 4. The lemma above can be easily generalized to any characteristic p, in this case the order of κ_a would be p.

Remark 5. It is well known that a square matrix is unipotent if and only if its characteristic polynomial $P(t)$ is a power of $t - 1$, i.e. it has a unique eigenvalue equals to 1.

We recall the following definition.

Definition 2. *Let A be an $n \times n$ matrix over a field $\mathbb{F}$, with $\lambda \in \mathbb{F}$ along the main diagonal and 1 along the diagonal above it, that is*

$$A = \begin{bmatrix} \lambda & 1 & \dots & 0 \\ 0 & \lambda & 1 \dots & 0 \\ \vdots & & & \vdots \\ 0 \dots & & & \lambda \end{bmatrix}.$$

Then A is called the $n \times n$ elementary Jordan matrix or Jordan block of size n.

Definition 3. *A matrix A defined over a field $\mathbb{F}$ is said to be in Jordan canonical form if A is block-diagonal where each block is a Jordan block defined over $\mathbb{F}$.*

The following theorem is well-known (see for instance [7]).

Theorem 2. *Let A be an $n \times n$ matrix over a field $\mathbb{F}$ such that any eigenvalue of A is contained in $\mathbb{F}$, then there exists a matrix J defined over $\mathbb{F}$, which is in Jordan canonical form and similar to A.*

Lemma 5. *Let $T_\circ \subseteq \mathrm{AGL}(V, +)$. Then for each $a \in V$, κ_a fixes at least $2^{\lfloor \frac{n-1}{2} \rfloor + 1}$ elements of V.*

Proof. From Lemma 4, κ_a has a unique eigenvalue equals to $1 \in \mathbb{F}_2$, then from Theorem 2 there exists a matrix over $\mathbb{F}_2$ in the Jordan form similar to κ_a. Thus, $\kappa_a = AJA^{-1}$, for some $A, J \in GL(V, +)$ with

$$
J = \begin{bmatrix}
1 & \alpha_1 & & \ldots & & 0 \\
0 & 1 & \alpha_2 & \ldots & & 0 \\
\vdots & & & & & \vdots \\
0 & \ldots & & 1 & \alpha_{n-1} & \\
0 & \ldots & & & & 1
\end{bmatrix}
\text{ and } J^2 = \begin{bmatrix}
1 & 0 & \alpha_1\alpha_2 & & \ldots & & 0 \\
0 & 1 & 0 & \alpha_2\alpha_3 & \ldots & & 0 \\
\vdots & & & & & & \vdots \\
0 & \ldots & & & 1 & 0 & \alpha_{n-2}\alpha_{n-1} \\
0 & \ldots & & & & 1 & 0 \\
0 & \ldots & & & & & 1
\end{bmatrix}.
$$

where $\alpha_i \in \mathbb{F}_2$ for $1 \leq i \leq n-1$.

From the fact that J is conjugated to κ_a we have $J^2 = 1_V$, and that implies $\alpha_i \alpha_{i+1} = 0$ for all $1 \leq i \leq n-2$.

Note that if $\alpha_i = 1$ then α_{i-1} and α_{i+1} have to be equal to 0. Thus we have that when n is even at most $\frac{n}{2}$ α_i's can be equal to 1. Then at least $\frac{n}{2}$ elements of the canonical basis are fixed by J. When n is odd we have at most $\frac{n-1}{2}$ α_i's equal to 1 and then at least $\frac{n-1}{2} + 1$ elements of the canonical basis are fixed by J. Our claim follows from the fact that κ_a is conjugated to J. $\qed$

In terms of algebras we have the following corollary.

Corollary 1. *Let $T_\circ \subseteq \mathrm{AGL}(V, +)$, and let $(V, +, \cdot)$ be the associated algebra of Theorem 1. Then for each $a \in V$, $a \cdot x$ is equal to 0 for at least $2^{\lfloor \frac{n-1}{2} \rfloor + 1}$ elements x of V.*

Remark 6. The bound on the number of elements fixed by κ_a given in Lemma 5 is tight. In fact let $(V, +, \cdot)$ be the exterior algebra over a vector space of dimension three, spanned by e_1, e_2, e_3. That is, V has basis

$$e_1, e_2, e_3, e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3, e_1 \wedge e_2 \wedge e_3.$$

We have that $e_1 \cdot x = 0$ for all $x \in E = \langle e_1, e_1 \wedge e_2, e_1 \wedge e_3, e_1 \wedge e_2 \wedge e_3 \rangle$. So, for all $x \in E$

$$x \circ e_1 = x + e_1 + x \cdot e_1 = x + e_1.$$

Vice versa if $x \circ e_1 = x + e_1$ then $x \in E$. The size of E is 2^4.

Lemma 6. *Let $T_\circ \subseteq \mathrm{AGL}(V,+)$. Then $f \in \mathrm{AGL}(V,\circ)$ is at least $2^{\lfloor \frac{n-1}{2} \rfloor + 1}$ differentially uniform.*

Proof. From Lemma 1 there exists $a \in U(T_\circ)$ different from zero. So

$$f(x+a) + f(x) = f(x \circ a) + f(x) = (f(x) \circ f(a)) + f(x) =$$

$$(f(x) + f(a) + f(a) \cdot f(x)) + f(x)$$

Now, from Corollary 1 we have that $f(a) \cdot f(x) = 0$ for at least $2^{\lfloor \frac{n-1}{2} \rfloor + 1}$ elements of V.
This implies $|\{x \mid f(x+a) + f(x) = f(a)\}| \geq 2^{\lfloor \frac{n-1}{2} \rfloor + 1}$.

Lemma 7. *Let $T_+ \subseteq \mathrm{AGL}(V,\circ)$. Then $f \in \mathrm{AGL}(V,\circ)$ is at least $2^{\lfloor \frac{n-1}{2} \rfloor + 1}$ differentially uniform.*

Proof. Note that Theorem 1, Lemma 1 and Corollary 1 hold also inverting the operation $\circ$ and $+$. Then, there exists $a \in V$ different from zero such that $x + a = x \circ a$ for all $x \in V$. Considering the algebra $(V, \circ, \cdot)$ such that $x + y = x \circ y \circ x \cdot y$ for all $x, y \in V$, we have

$$f(x+a) + f(x) = f(x \circ a) + f(x) = (f(x) \circ f(a)) + f(x) =$$

$$(f(x) \circ f(a)) \circ f(x) \circ f(x) \cdot (f(x) \circ f(a)) =$$

$$f(x) \circ f(a) \circ f(x) \circ f(x) \cdot f(x) \circ f(x) \cdot f(a).$$

From Remark 2, we have $y^2 = 0$ for all $y \in V$, and from Corollary 1 $f(x) \cdot f(a) = 0$ for at least $2^{\lfloor \frac{n-1}{2} \rfloor + 1}$ elements. Thus

$$|\{x \mid f(x+a) + f(x) = f(a)\}| \geq 2^{\lfloor \frac{n-1}{2} \rfloor + 1}.$$

Summarizing our results in this section, especially Lemma 2, 3, 6, 7, we obtain our theorem on the claimed differentiability.

Theorem 3. *Let $T_\circ \subseteq \mathrm{AGL}(V,+)$ $(T_+ \subseteq \mathrm{AGL}(V,\circ)$, respectively). Let $f \in \mathrm{AGL}(V,\circ)$. Then $\delta(f) \geq 2^m$, where*

- $m = \max\{\lfloor \frac{n-1}{2} \rfloor + 1, \dim(U(T_\circ))\}$
- $(m = \max\{\lfloor \frac{n-1}{2} \rfloor + 1, \dim(U_\circ(T_+))\}$, *respectively).*

By a computer check we obtain the following fact.

Fact 1 *Let $V = \mathbb{F}_2^n$ with $n = 3, 4, 5$. If $T_+ \subseteq \mathrm{AGL}(V,\circ)$, let $f \in \mathrm{AGL}(V,\circ)$. Then $\delta(f) \geq 2^{n-1}$.*

Remark 7. For $n = 7, 8$ there exist examples of functions that are affine w.r.t. a hidden sum $\circ$ satisfying $T_+ \subseteq \mathrm{AGL}(V, \circ)$ and $\delta(f) = 2^{n-2}$. The existence of these permutations and Fact 1 suggest that probably there may exist bounds which are sharper than those in Theorem 3.

Remark 8. Note that if we consider $f \in \mathrm{Sym}(\mathbb{F}_2^4)$ with $\delta(f) = 4$ then the parallel map (f, f) acting on $\mathbb{F}_2^8$ is 2^6 differentially uniform. Thus the differential uniformity may not guarantee, alone, security from a hidden sum trapdoor!

4   A block cipher with a hidden sum

In this section we give an example, similar to that described in [1], of a translation based block cipher in a small dimension, in which it is possible to embed a hidden-sum trapdoor.

Let $m = 3$, $n = 2$, then $d = 6$ and we have the message space $V = \mathbb{F}_2^6$. The mixing layer of our toy cipher is given by the matrix

$$\lambda = \begin{bmatrix} 0\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1 \\ 0\,0\,0\,0\,0\,1 \\ 1\,0\,1\,0\,0\,1 \\ 1\,1\,1\,0\,0\,1 \\ 0\,0\,1\,0\,0\,0 \end{bmatrix}$$

Note that λ is a proper mixing layer (see Definition 3.2 [2]). The bricklayer transformation $\gamma = (\gamma_1, \gamma_2)$ of our toy cipher is given by two identical S-boxes

$$\gamma_1 = \gamma_2 = \alpha^4 x^6 + \alpha^3 x^4 + \alpha x^3 + \alpha^3 x^2 + x + \alpha^6$$

where α is a primitive element of $\mathbb{F}_{2^3}$ such that $\alpha^3 = \alpha + 1$.
The S-box γ_1 is 4-differential uniform.

Consider the hidden sum $\circ$ over $V_1 = V_2 = (\mathbb{F}_2)^3$ induced by the elementary abelian regular group $T_\circ = \langle \tau_1, \tau_2, \tau_3 \rangle$, where

$$\tau_1(x) = x \cdot \begin{bmatrix} 1\,0\,0 \\ 0\,1\,1 \\ 0\,0\,1 \end{bmatrix} + e_1, \ \tau_2(x) = x \cdot \begin{bmatrix} 1\,0\,1 \\ 0\,1\,0 \\ 0\,0\,1 \end{bmatrix} + e_2, \ \tau_3(x) = x \cdot \begin{bmatrix} 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{bmatrix} + e_3,$$

$$\tag{1}$$

with $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ and $e_3 = (0, 0, 1)$. In other words, $\tau_i(x) = x \circ e_i$ for any $1 \leq i \leq 3$.

Obviously $T = T_\circ \times T_\circ$ is an elementary abelian group inducing the hidden sum $(x_1, x_2) \circ' (y_1, y_2) = (x_1 \circ y_1, x_2 \circ y_2)$ on $V = V_1 \times V_2$. By a computer check it results $\langle T_+, \lambda\gamma \rangle \subseteq \mathrm{AGL}(V, \circ')$, and $\circ'$ is a hidden sum for our toy cipher. It remains to verify whether it is possible to use it to attack the toy cipher with an attack that costs less than brute force. We are considering a cipher where the number of rounds is so large to make any classical attack useless (such as differential cryptanalysis) and the key scheduling offer no weakness. Therefore, the hidden sum will actually be essential to break the cipher only if the attack that we build will cost significantly less than 64 encryptions, considering that the key space is $\mathbb{F}_2^6$.

Remark 9. $T_\circ$ is generated by the translations corresponding to e_1, e_2 and e_3, which implies that the vectors e_1, e_2, e_3 form a basis for $(V_1, \circ)$. Let $x = (x_1, x_2, x_3) \in V_1$, from (1) we can simply write

$$\tau_1(x) = (x_1 + 1, x_2, x_2 + x_3), \tau_2(x) = (x_1, x_2 + 1, x_1 + x_3), \tau_3(x) = (x_1, x_2, x_3 + 1).$$

Let us write x as a linear combination of e_1, e_2 and e_3 w.r.t. to the sum $\circ$, i.e. $x = \lambda_1 e_1 \circ \lambda_2 e_2 \circ \lambda_3 e_3$. We have that $\lambda_1 = x_1$, $\lambda_2 = x_2$ and $\lambda_3 = \lambda_1 \lambda_2 + x_3$. So

$$(x_1, x_2, x_3) = x = (\lambda_1, \lambda_2, \lambda_1 \lambda_2 + \lambda_3) \tag{2}$$

Thanks to the previous remark we can find the coefficients of a vector $v' = (v, u) \in V$ with respect to $\circ'$ by using the following algorithm separately on the two bricks of v'.

Algorithm 1
Input: *vector $x \in \mathbb{F}_2^3$*
Output: *coefficients λ_1, λ_2 and λ_3.*
[1] $\lambda_1 \leftarrow x_1$;
[2] $\lambda_2 \leftarrow x_2$;
[3] $\lambda_3 \leftarrow \lambda_1 \lambda_2 + x_3$;
return $\lambda_1, \lambda_2, \lambda_3$.

Let $v' = (v, u) \in V$, we write

$$v = \lambda_1^v e_1 \circ \lambda_2^v e_2 \circ \lambda_3^v e_3 \text{ and } u = \lambda_1^u e_1 \circ \lambda_2^u e_2 \circ \lambda_3^u e_3.$$

We denote by

$$[v'] = [\lambda_1^v, \lambda_2^v, \lambda_3^v, \lambda_1^u, \lambda_2^u, \lambda_3^u]$$

the vector with the coefficients obtained from the bricks of v' using Algorithm 1.

Let $\varphi = \varphi_k$ be the encryption function, with a given unknown session key k. We want to mount two attacks by computing the matrix M and the translation vector t defining $\varphi \in \mathrm{AGL}(V, \circ')$, so $t = \varphi(0)$ and $[\varphi(x)] = [x] \cdot M + [t]$.

Assume we can call the encryption oracle. Then M can be computed from the 7 ciphertexts $\varphi(0), \varphi(e_1'), \ldots, \varphi(e_6')$ (where $e_1' = (1, 0, 0, 0, 0, 0), \ldots, e_6' = (0, 0, 0, 0, 0, 1)$), since the $([\varphi(e_i')] + [t])$'s represent the matrix rows. In other words, we will have

$$[\varphi(v')] = [v'] \cdot M + [t], \quad [\varphi^{-1}(v')] = ([v'] + [t]) \cdot M^{-1},$$

for all $v' \in V$, where the product row by column is the standard scalar product. The knowledge of M, t and M^{-1} provides a global deduction (reconstruction), since it becomes trivial to encrypt and decrypt. In fact, to encrypt v it is enough to compute $[v]$, applying $[v] \mapsto [v] \cdot M + [t] = [w]$ and then pass from $[w]$ to the standard representation w via (2). Analogously to decrypt. However, following [1], we have an alternative depending on how we compute M^{-1}, resulting in one attack with 7 encryptions and another with 7 encryptions and 7 decryptions. Both are much faster than brute-force searching in the keyspace.

References

1. R. Aragona, M. Calderini, and M. Sala. *The role of Boolean functions in hiding sums as trapdoors for some block ciphers*, arXiv preprint arXiv:1411.7681 (2014).
2. R. Aragona, A. Caranti, F. Dalla Volta, M. Sala, *On the group generated by the round functions of translation based ciphers over arbitrary finite fields*, Finite Fields and Their Applications 25 (2014), 293–305.
3. E. Biham, A.Shamir *Differential cryptanalysis of DES-like cryptosystems*. J. Cryptol 4(1) (1991), 3–72.
4. 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.
5. A. Caranti, F. Dalla Volta, and M. Sala, *An application of the ONan-Scott theorem to the group generated by the round functions of an AES-like cipher*, Designs, Codes and Cryptography 52 (2009), no. 3, 293–301.
6. A. Caranti, F. Dalla Volta, and M. Sala, *On some block ciphers and imprimitive groups*, AAECC 20 (2009), no. 5-6, 229–350.
7. S. Lang, *Linear Algebra*. Springer Undergraduate Texts in Mathematics and Technology. Springer, (1987).
8. Cai Heng Li, *The finite primitive permutation groups containing an abelian regular subgroup*, Proceedings of the London Mathematical Society 87 (2003), no. 03, 725–747.
9. M. Calderini *On Boolean functions, symmetric cryptography and algebraic coding theory*, Ph.D. thesis, University of Trento (2015).
10. K. Nyberg, *Differentially uniform mappings for cryptography*, Advances in Cryptology, EUROCRYPT '93, Lecture Notes in Computer Science 765 (1994), 55–64.

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