On the groups of alternative operations for differential cryptanalysis

Riccardo Aragona, Roberto Civino, Norberto Gavioli, and Carlo Maria Scoppola

DISIM - University of L'Aquila
riccardo.aragona@univaq.it, roberto.civino@univaq.it,
norberto.gavioli@univaq.it, scoppola@univaq.it

Abstract In a recent paper, Civino et al. considered alternative operations to mount a differential attack against a block cipher. Such operations are different from the one used to perform the round-key addition, and are induced by elementary abelian regular subgroups of the symmetric group acting on the plaintext space. It has been shown on a small cipher how a successful attack can be mounted, even in the in case the cipher is designed to be resistant to the classical attack. In view of the potential interest for the application in cryptanalysis, here we study the relationships between a class of elementary abelian regular subgroups and the Sylow 2-subgroups of their normalisers in the symmetric group $\mathrm{Sym}(\mathbb{F}_2^n)$ and their cryptographic implications.

The results contained in this extended abstract are included in a paper by the same authors submitted to a journal.

Keywords: block ciphers, differential cryptanalysis, alternative operations, group theory, affine groups.

1 Introduction and motivation

Let $n > 2$ and let $(V, +)$ be an n-dimensional vector space over the field with two elements, where $+$ denotes the bitwise XOR operation. The conjugacy class of elementary abelian regular subgroups of the symmetric group $\mathrm{Sym}(V)$ has recently drawn the attention of researchers in symmetric cryptography [CDVS06, CS17, BCS19], as these subgroups and their normalisers (i.e. isomorphic copies of the affine group) may be used to detect weaknesses in some symmetric-encryption methods, i.e. block ciphers. More specifically, cryptanalysts may take advantage of the alternative operations that these groups induce on the plaintext space and exploit them to detect biases in the distribution of the ciphertexts by means of techniques of differential cryptanalysis [CBS18].

A block cipher on the plaintext space V is a family $\{ E_k \}_{k \in \mathcal{K}}$ of non-linear permutations of $\mathrm{Sym}(V)$, called *encryption functions*, indexed by a set of parameters $\mathcal{K}$, called *keys*. Each encryption function is in general obtained as the composition of different layers (non-linear *confusion layers*, linear *diffusion layers*,

and affine *key-addition layers*), each one designed with a precise cryptographic goal, depending on its role in the employed algorithm (see e.g. [DR13, BKL+07, NBoS77]). Some of those layers usually provide entropy to the encryption process by means of bit-wise XOR addition with *round keys* in V computed by a public procedure, called *key schedule*, starting from the user-selected key in $\mathcal{K}$. The non-linearity of the functions E_k is one of the crucial requirements to provide security against a large variety of statistical attacks, such as differential [BS91] and linear [Mat93] cryptanalysis. For this reason, ways of making the cipher's components as far as possible from being linear are extensively studied [Nyb93]. The usually considered notion of non-linearity is given with respect to the operation which is used in the cipher to perform the key addition, and the security of a cipher depends, among other things, on the requirement that its encryption functions do not behave as affine functions, i.e. they lie far from $\mathrm{AGL}(V)$, the group of affine functions on V. However, several isomorphic copies of $\mathrm{AGL}(V)$ are contained in $\mathrm{Sym}(V)$, and each of them corresponds to a different operation endowing V with a distinct vector space structure. In a more concrete way, using the terminology of differential cryptanalysis, the fact that the key-addition is XOR-based does not force an attacker to use the XOR as the operation defining differentials. As a matter of fact, nothing guarantees that the differential probabilities computed with respect to the XOR are higher than those computed with respect to different operations, and hence that the security from XOR-based differential attacks implies the immunity from differential attacks induced by whatever difference operator [CBS18]. For this reason, a target of a new branch of research in symmetric cryptography [CDVS06, CS17, CBS18, BCS19] is to investigate the non-linearity of the encryption functions of a cipher with respect to these alternative operations. In the remainder of the paper the use of these operations for differential cryptanalysis is quickly discussed (Sec. 2), and it is pointed out that a specific class of them is optimal. Such a class needs a thorough study, which is the aim of this paper. Some novel contributions are listed in Sec. 3. The study of the groups of Sec. 3, moreover, allowed us to derive some general properties of the affine group and its Sylow 2-subgroups, which are presented in Sec. 4. Such results are relevant both for their implications in cryptanalysis as well as from a purely group theoretical point of view.

2 New operations for cryptanalysis

Here and in the remainder of the paper we use the postfix notation for functional evaluations, i.e. if G is a group acting on V and x in an element of V, we write xg to mean $g(x)$.

Let $T \stackrel{\text{def}}{=} \{\, \sigma_v \mid v \in V,\, x \mapsto x + v \,\} < \mathrm{Sym}(V)$ be the group of translations with respect to the XOR. Notice that the function σ_k acts on the message $x \in V$ as a key-addition layer, i.e. $x\sigma_k = x + k$. Every conjugate T^g of T, where $g \in \mathrm{Sym}(V)$, defines another operation $\circ$ on V. This is easily done by letting

$$\forall u, v \in V \quad u \circ v \stackrel{\text{def}}{=} u\tau_v,$$

where τ_v is the unique map in T^g for which $0 \mapsto v$. For reasons that will be clear soon, the set

$$W_\circ \stackrel{\text{def}}{=} \{k \mid k \in V, \forall x \in V \; x + k = x \circ k\} \cong T \cap T^g \tag{1}$$

is crucial. It is called the *weak-key subspace*, its elements are called *weak keys*, and a straightforward check shows that $W_\circ$ is a subspace of both $(V, +)$ and $(V, \circ)$. In the context of differential cryptanalysis the knowledge of $W_\circ$ plays an important role, since it represents the set of round keys for which the XOR-addition with every message and the $\circ$-addition give the same result. In another way, if the round-key is a weak key, differentials with respect to $\circ$ propagate through the key-addition layer as differentials with respect to $+$ do.

Notice that, in view of the identification of Eq. (1), if $g \in \mathrm{Sym}(V)$ is the element inducing the operation $\circ$ by conjugation, for sake of simplicity we may also write $T \cap T^g$ and $\dim(T \cap T^g)$ to mean $W_\circ$ and $\dim(W_\circ)$ respectively. The following result gives a bound on the dimension of the weak-key space.

Proposition 1. *If $g \in \mathrm{Sym}(V)$ such that $T \neq T^g$, then $\dim(T \cap T^g) \leq n - 2$.*

Proof. Let $W_\circ$ be the weak-key space of the operation induced by the group T^g, and assume by way of contradiction that $\dim(W) = n - 1$. Let $\{ v_i \}_{i=1}^{n-1}$ be a basis for $W_\circ$ and $v \in V \setminus W_\circ$. The claim holds if $a\tau_v = a\sigma_v$ for any $a \in V$. If $a \in W_\circ$ there is nothing to prove, hence without loss of generality we may assume $a = w + v$, for some $w \in W_\circ$. Then

$$\begin{aligned} a\tau_v &= (w + v)\tau_v = (w\sigma_v)\tau_v \\ &= (w\tau_v)\tau_v = w(\tau_v)^2 = w \\ &= a\sigma_v. \end{aligned}$$

□

In [CBS18] the problem of the construction of alternative operations is investigated and several examples are provided. In one of those, the obtained operation is used to mount a differential attack against a 15-bit Substitution-Permutation Network, whose 3-bit S-boxes are 2-differentially uniform [Nyb93] with respect to the XOR and 8-differentially uniform with respect to the new operation. The success of the attack relies on the aforementioned fact, since the non-linearity of the confusion layer is highly weakened, as well as on the fact that the provided diffusion layer is a linear function with respect to both the operation considered. This allows the differentials computed with respect to $\circ$ to pass through the diffusion layer in a deterministic way. However, when the chosen operation is different from the XOR, used to add the key in the different rounds of the cipher, differential probabilities have to be introduced when studying the interaction between $\circ$-differences and the key-addition layer. For this reason, in order to make the attack successful a last step is required, i.e. providing condition granting that $\circ$-differential probabilities are as high as possible. It has been

shown in [CBS18] that the size of those probability depends on the dimension of $W_\circ$ as a subspace of V, and in particular the highest values are obtained when $\dim(W_\circ) = n-2$, the upper bound of Proposition 1. For now on we concentrate on operations with such a property, considering the family of *second-maximal-intersection subgroups* of $\mathrm{Sym}(V)$, i.e. the families of elementary abelian regular subgroups of $\mathrm{Sym}(V)$ that intersect T in a subgroup of order 2^{n-2}.

3 Second-maximal-intersection subgroups

As we mentioned earlier, these last sections are devoted to the study of second-maximal-intersection subgroups, in view of their application in differential attacks of block ciphers. As a first important result, we prove that elementary abelian regular subgroups that intersect T in a second-maximal subgroup are all made by affinities.

Theorem 1. *Let $g \in \mathrm{Sym}(V)$. If $\dim(T \cap T^g) = n-2$, then $T^g < \mathrm{AGL}(V)$.*

The importance of this result is substantial for its application to cryptanalysis. Indeed, let $T^g = \{\tau_v \mid v \in V\}$ be a second-maximal-intersection subgroup. Theorem 1 implies that for each $v \in V$ there exists an invertible binary matrix M_v such that $\tau_v = M_v \sigma_v$. Hence, once a basis $\{v_i\}_{i=1}^n$ of V is fixed, the operation $\circ$ can be computed simply storing the n invertible binary matrix M_{v_i}, for $1 \leq i \leq n$, making the computation efficient even in the case of a real-life-size block ciphers. An explicit description of such matrices with respect to the canonical basis of V is provided next in Proposition 2.

Remark 1. In the hypotheses of Theorem 1, by interchanging the roles of T and T^g, one can easily obtain that also T is a subgroup of $\mathrm{AGL}(V)^g$. Notice that $\mathrm{AGL}(V)^g$ represents the group of affine functions with respect to $\circ$ induced by T^g. As shown in [CBS18], the previous property makes the key-addition layer of the cipher an affine function with respect to $\circ$, which is crucial in view of maximising the $\circ$-differential probabilities in a differential attack.

In order to give a complete description of second-maximal-intersection subgroups, it is convenient to give a more practical representation. To this purpose, let us assume that $W_\circ$ is spanned by the last $n-2$ vectors of the canonical basis $\{e_i\}_{i=1}^n$ of V. The next result gives a parametrisation and counts the number of subgroups with such a property.

Proposition 2. *Let $W \stackrel{\text{def}}{=} \langle e_i \mid 3 \leq i \leq n \rangle$. The group $\mathrm{Sym}(V)$ contains $2^{n-2}-1$ elementary abelian regular subgroups T_b, indexed by $b \in W \setminus \{0\}$, such that $T \cap T_b = W$. More precisely, $T_b = \langle \pi_b, \varepsilon_b, \sigma_{e_i} \mid 3 \leq i \leq n \rangle$, where*

$$\pi_b = \left(\begin{array}{c|c} 1_2 & \begin{matrix} 0 \\ b^{(3:n)} \end{matrix} \\ \hline 0 & 1_{n-2} \end{array}\right) \sigma_{e_1}, \quad \varepsilon_b = \left(\begin{array}{c|c} 1_2 & \begin{matrix} b^{(3:n)} \\ 0 \end{matrix} \\ \hline 0 & 1_{n-2} \end{array}\right) \sigma_{e_2}. \tag{2}$$

The general problem of parametrising all the elementary abelian regular subgroups T^g of $\mathrm{Sym}(V)$ and of $\mathrm{AGL}(V)$ according to the size of their intersection with T is not easy in general. Proposition 2 solves this problem in the case of second-maximal-intersection subgroups. Partial results have been obtained in the case $T^g < \mathrm{AGL}(V)$ [CS17, CBS18, BCS19]. In [CS17] a result similar to the following corollary is proved, where $\mathrm{AGL}(V)$ appears in place of $\mathrm{Sym}(V)$. The present form is a consequence of Theorem 1 and the result is easily derived by Proposition 2.

Corollary 1. *The group* $\mathrm{Sym}(V)$ *contains* t_n *elementary abelian regular subgroups whose intersection with* T *is a second-maximal subgroup of* T*, where*

$$t_n \stackrel{\text{def}}{=} \frac{\left(2^{n-2}-1\right)\left(2^{n-1}-1\right)\left(2^n-1\right)}{3}.$$

Proof. The integer t_n may be obtained as the product of $2^{n-2}-1$ and $(2^n-1)(2^n-2)/6$, respectively the number of elementary abelian regular subgroups which intersect T in the subspace spanned by the last $n-2$ vectors of the canonical basis and the number of $(n-2)$-dimensional subspaces of V. □

4 On the Sylow 2-subgroups of AGL(V)

In this section, using the contributions of Sec. 3 we establish some algebraic results on the affine group looking at its Sylow 2-subgroups and the way they contain second-maximal-intersection subgroups.

Theorem 2. *Every Sylow* 2*-subgroup* Σ *of* $\mathrm{AGL}(V)$ *contains exactly one elementary abelian regular subgroup* T_Σ *intersecting* T *in a second-maximal subgroup of* T *and which is normal in* Σ*.*

The previous theorem has the following converse. The same notation is used.

Proposition 3. *If* $\bar{T}$ *is an elementary abelian regular subgroup of* $\mathrm{AGL}(V)$ *such that* $\left|\bar{T}\cap T\right| = 2^{n-2}$*, then there exists a Sylow* 2*-subgroup* Σ *of* $\mathrm{AGL}(V)$ *such that* $\bar{T} = T_\Sigma \trianglelefteq \Sigma$*.*

We prove in Theorem 3 that if a Sylow 2-subgroup Σ of $\mathrm{AGL}(V)$ contains a conjugate in $\mathrm{Sym}(V)$ of T as a normal subgroup, then such a subgroup is either T or T_Σ, where T_Σ is as in Theorem 2.

Theorem 3. *Let* $g \in \mathrm{Sym}(V)$ *and let* Σ *be a Sylow* 2*-subgroup of* $\mathrm{AGL}(V)$ *containing* T^g*. The subgroup* T^g *is normal in* Σ *if and only if* $T^g \in \{T, T_\Sigma\}$*.*

From Theorem 3 we can also conclude that second-maximal-intersection subgroups are characterised by the fact that their normalisers contain a Sylow 2-subgroup of $\mathrm{AGL}(V)$.

Corollary 2. *Let $g \in \mathrm{Sym}(V) \setminus \mathrm{AGL}(V)$ such that T^g is an elementary abelian regular subgroup of $\mathrm{Sym}(V)$. If $|\,\mathrm{AGL}(V)\,| = 2^m t$, with t an odd integer, then*

$$|\,T \cap T^g\,| = 2^{n-2} \iff 2^m \mid |\,\mathrm{AGL}(V) \cap \mathrm{AGL}(V)^g\,|\,.$$

Proof. If $|\,T \cap T^g\,| = 2^{n-2}$, then by Theorem 1, both T and T^g are subgroups of $\mathrm{AGL}(V)$. Moreover, since T is contained in every Sylow 2-subgroup of $\mathrm{AGL}(V)$, at least one of them, which we denote by Σ, contains both T and T^g as normal subgroups. Thus $\Sigma \leq \mathrm{AGL}(V) \cap \mathrm{AGL}(V)^g$. Conversely, if this is the case, T and T^g, being contained in every Sylow 2-subgroup of their own normalisers, are distinct normal subgroups of Σ. Therefore, Theorems 2 and 3 yield $\{\,T, T^g\,\} = \{\,T, T_\Sigma\,\}$, hence $|\,T \cap T^g\,| = 2^{n-2}$. □

The previous result is important in view of its cryptographic application, since $\mathrm{AGL}(V)^g$ represent the group of affine functions with respect to the operation $\circ$ induced by T^g. So the group $\mathrm{AGL}(V) \cap \mathrm{AGL}(V)^g$ contains as a subgroup the group of all the invertible binary matrices which are linear with respect to both the operations, which can be used to select a suitable diffusion layer for a trapdoor cipher.

The last contributions of this section, which are derived from the previous results on elementary abelian regular subgroups for cryptography, are important for their group-theoretical relevance. It was already known to P. Hall (see e.g. [CF64]) that if Ξ is a Sylow 2-subgroup of $\mathrm{Sym}(V)$, then $N_{\mathrm{Sym}(V)}(\Xi) = \Xi$. In the remainder of the paper we establish a similar result for Sylow 2-subgroups of $\mathrm{AGL}(V)$.

Theorem 4. *If Σ is a Sylow 2-subgroup of $\mathrm{AGL}(V)$, then*

$$[N_{\mathrm{Sym}(V)}(\Sigma) : \Sigma] = 2.$$

The result which follows is the counterpart in $\mathrm{AGL}(V)$ of the result due to P. Hall on the Sylow 2-subgroups of $\mathrm{Sym}(V)$. It also allows us to count the number of distinct Sylow 2-subgroups of $\mathrm{AGL}(V)$.

Theorem 5. *If Σ is Sylow 2-subgroup of $\mathrm{AGL}(V)$, then $N_{\mathrm{AGL}(V)}(\Sigma) = \Sigma$. In particular,*

$$[\mathrm{AGL}(V) : \Sigma] = \prod_{j=0}^{n-1} \left(2^{n-j} - 1\right). \tag{3}$$

is the number of distinct Sylow 2-subgroups of $\mathrm{AGL}(V)$.

Proof. By Theorem 4, if $|\,\mathrm{AGL}(V)\,| = 2^m t$, with t an odd integer, then we have $|\,\Sigma\,| = 2^m$ and $\left|\,N_{\mathrm{Sym}(V)}(\Sigma)\,\right| = 2^{m+1}$. Since $N_{\mathrm{AGL}(V)}(\Sigma) \leq \mathrm{AGL}(V)$ and $N_{\mathrm{AGL}(V)}(\Sigma) \leq N_{\mathrm{Sym}(V)}(\Sigma)$, then $\left|\,N_{\mathrm{AGL}(V)}(\Sigma)\,\right| = 2^m$. □

Corollary 3. *The number s_n of Sylow 2-subgroups of $\mathrm{AGL}(V)$ which contain as a normal subgroup the same group T^g such that $\dim(W) = n-2$, where $\sigma_W = T \cap T^g$ and $g \in \mathrm{Sym}(V)$, is given by the formula:*

$$s_n = 3 \prod_{j=3}^{n-1} \left(2^{n-j} - 1\right).$$

Proof. Let $|\,\mathrm{AGL}(V)\,| = 2^m t$, with t an odd integer. First we recall that t is the integer displayed in Eq. (3). The claim follows from Corollary 1, since $s_n = t/t_n$, where t_n is the number of elementary abelian regular subgroups in $\mathrm{AGL}(V)$ whose intersection with T is a second-maximal subgroup of T. □

5 Conclusion and open problems

We already mentioned that the conjugates in $\mathrm{Sym}(V)$ of T are very important in the cryptanalysis of block ciphers. For this reason, a complete parametrisation of them in terms of the size of their intersection with T is needed. Recall that the elements of such intersections are in one-to-one correspondence with the weak keys corresponding to the alternative operations. In this paper, the aforementioned problem has been addressed in the case where the weak-key subspace has dimension $n-2$. This last case turned out to be one of the most relevant for cryptanalysis, since the corresponding operations may be used to perform a differential attack [CBS18]. We have computational evidence that also the case of lower dimensional weak-key spaces might be interesting from a cryptographic point of view, though it may require an entirely different technical approach.

Bibliography

[BCS19] Carlo Brunetta, Marco Calderini, and Massimiliano Sala, *On hidden sums compatible with a given block cipher diffusion layer*, Discrete Mathematics **342** (2019), no. 2, 373–386.

[BKL+07] Andrey Bogdanov, Lars R Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, and Charlotte Vikkelsoe, *PRESENT: An ultra-lightweight block cipher*, International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2007, pp. 450–466.

[BS91] Eli Biham and Adi Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Journal of CRYPTOLOGY **4** (1991), no. 1, 3–72.

[CBS18] Roberto Civino, Céline Blondeau, and Massimiliano Sala, *Differential attacks: using alternative operations*, Designs, Codes and Cryptography (2018).

[CDVS06] Andrea Caranti, Francesca Dalla Volta, and Massimiliano Sala, *Abelian regular subgroups of the affine group and radical rings*, Publ. Math. Debrecen **69** (2006), no. 3, 297–308. MR 2273982

[CF64] Roger Carter and Paul Fong, *The Sylow* 2*-subgroups of the finite classical groups*, J. Algebra **1** (1964), 139–151. MR 0166271

[CS17] Marco Calderini and Massimiliano Sala, *Elementary abelian regular subgroups as hidden sums for cryptographic trapdoors*, ArXiv e-prints (2017).

[DR13] Joan Daemen and Vincent Rijmen, *The design of Rijndael: AES-the advanced encryption standard*, Springer Science & Business Media, 2013.

[Mat93] Mitsuru Matsui, *Linear cryptanalysis method for DES cipher*, Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1993, pp. 386–397.

[NBoS77] US Department of Commerce National Bureau of Standards, *Data encryption standard*, Federal information processing standards publication 46 **23** (1977).

[Nyb93] Kaisa Nyberg, *Differentially uniform mappings for cryptography*, Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1993, pp. 55–64.