A NOTE ON SOME ALGEBRAIC TRAPDOORS FOR BLOCK CIPHERS

MARCO CALDERINI
Department of Mathematics, University of Trento, Italy

Abstract. We provide sufficient conditions to guarantee that a translation based cipher is not vulnerable with respect to the partition-based trapdoor. This trapdoor has been introduced, recently, by Bannier et al. (2016) and it generalizes that introduced by Paterson in 1999. Moreover, we discuss the fact that studying the group generated by the round functions of a block cipher may not be sufficient to guarantee security against these trapdoors for the cipher.

1. Introduction. In the last years, since the work [7] of Coppersmith and Grossman, much attention has been devoted to the group generated by the round functions of a block cipher. In this context, Paterson [9] showed that the imprimitivity of the group can be exploited to construct a trapdoor. By a trapdoor we mean a hidden algebraic structure in the cipher design that would allow an attacker (with the knowledge of the trapdoor) to break it easily. In [2] Caranti, Dalla Volta and Sala introduced the class of translation based ciphers, which contains well-known ciphers like AES [4], SERPENT [5] and PRESENT [6]. For this class of cipher, in [2] and [10], the authors provided cryptographic conditions on the S-Boxes and then mixing layer, in order to guarantee the primitivity of the group generated by the round functions of the cipher.

In a recent work [11], inspired by the partition cryptanalysis developed in [12], the authors introduce the partition-based trapdoor. This type of trapdoor generalizes that introduced by Paterson. Moreover, the authors give an example of a (toy) block cipher which is not vulnerable with respect to linear and differential attacks, but that can be broken, easily, using the structure of the trapdoor.

In this work, we give some conditions on the S-boxes and the mixing layer of a translation based cipher, in order to avoid this new trapdoor. From this result, we are able to give a security proof for the group of encryption functions of a cipher with independent round-keys. In fact, it may happen that the group generated by the round functions is considered secure, while the group of encryption functions with independent round-keys is not.

The paper is organized as follows. In Section 2, we recall some definitions and a series of properties and already known results. In Section 3, we show how we can avoid the partition-based trapdoor on a translation based cipher. Finally, in Section 4, we discuss the fact that studying the group generated by the round functions of

2010 Mathematics Subject Classification. Primary: 94A60, 20B15; Secondary: 20B35.
Key words and phrases. Cryptography, primitive group, block cipher, trapdoors, group generated by round functions.
Definition 2.2. Let $\mathcal{C}$ be a block cipher acting on a message space $V = (\mathbb{F}_2)^d$, for some $d \geq 1$ (we suppose that $V$ coincides with the ciphertext space). Let $\mathcal{K}$ be its key space. Then any key $k \in \mathcal{K}$ individuates a permutation $\tau_k$ on the space $V$ and our cipher is given by the set

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

We are interested in determining the properties of the group $\Gamma(\mathcal{C}) = \{ \tau_k \mid k \in \mathcal{K} \}$. Unfortunately, the study of $\Gamma(\mathcal{C})$ is a difficult task, in general. Most modern block ciphers are iterated ciphers, i.e., obtained by a composition of several key-dependent permutations, called rounds. This allows to investigate another permutation group related to $\mathcal{C}$. For an iterated block cipher $\mathcal{C}$ each $\tau_k$ is a composition of some permutations of $V$, say $\tau_{k,1}, \ldots, \tau_{k,\ell}$. For any round $h$, let

$$\Gamma_h(\mathcal{C}) = \{ \tau_{k,h} \mid k \in \mathcal{K} \},$$

therefore, we can define the group containing $\Gamma(\mathcal{C})$ generated by the round functions

$$\Gamma_\infty(\mathcal{C}) = \langle \Gamma_h(\mathcal{C}) \mid h = 1, \ldots, \ell \rangle.$$

2. Preliminaries and notation. Let $\mathcal{C}$ be a block cipher acting on a message space $V = (\mathbb{F}_2)^d$, for some $d \geq 1$ (we suppose that $V$ coincides with the ciphertext space). Let $\mathcal{K}$ be its key space. Then any key $k \in \mathcal{K}$ individuates a permutation $\tau_k$ on the space $V$ and our cipher is given by the set

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

We are interested in determining the properties of the group $\Gamma(\mathcal{C}) = \{ \tau_k \mid k \in \mathcal{K} \}$. Unfortunately, the study of $\Gamma(\mathcal{C})$ is a difficult task, in general. Most modern block ciphers are iterated ciphers, i.e., obtained by a composition of several key-dependent permutations, called rounds. This allows to investigate another permutation group related to $\mathcal{C}$. For an iterated block cipher $\mathcal{C}$ each $\tau_k$ is a composition of some permutations of $V$, say $\tau_{k,1}, \ldots, \tau_{k,\ell}$. For any round $h$, let

$$\Gamma_h(\mathcal{C}) = \{ \tau_{k,h} \mid k \in \mathcal{K} \},$$

therefore, we can define the group containing $\Gamma(\mathcal{C})$ generated by the round functions

$$\Gamma_\infty(\mathcal{C}) = \langle \Gamma_h(\mathcal{C}) \mid h = 1, \ldots, \ell \rangle.$$

2.1. Translation based ciphers. Here we consider translation based cipher, introduced in [2]. This class of iterated block ciphers includes some well-known ciphers, as for instance AES and SERPENT.

We first fix the notation, in order to recall the definition of a translation based cipher $\mathcal{C}$. Let $m, b > 1$ and

$$V = V_1 \oplus \cdots \oplus V_b,$$

where each $V_i$ are isomorphic to $(\mathbb{F}_2)^m$. We will denote by $\text{Sym}(V)$ the symmetric group on $V$. Given $v \in V$, we write $\sigma_v \in \text{Sym}(V)$ for the translation of $V$ mapping $x$ to $x + v$. We denote by $T(V)$ the group of all translations of $V$. We will write the action of $g \in \text{Sym}(V)$ on an element $v \in V$ as $vg$.

For any $v \in V$, we will write $v = v_1 \oplus \cdots \oplus v_b$, where $v_i \in V_i$. Also, we consider the projections $\pi_i : V \to V_i$ mapping $v \mapsto v_i$.

Any $\gamma \in \text{Sym}(V)$ that acts as $\gamma v = v_1 \gamma_1 \oplus \cdots \oplus v_b \gamma_b$, for some $\gamma_i \in \text{Sym}(V_i)$, is called bricklayer transformation (a “parallel map”) and any $\gamma_i$ is a brick. Traditionally, the maps $\gamma_i$’s are called S-boxes and $\gamma$ a “parallel S-box”. A linear map $\lambda : V \to V$ is traditionally said a “Mixing Layer” when used in composition with parallel maps. For any $I \subset \{1, \ldots, b\}$, with $I \neq \emptyset$ and $I \neq \{1, \ldots, b\}$, we define $\bigoplus_{i \in I} V_i$ a wall.

Definition 2.1. A linear map $\lambda \in \text{GL}(V)$ is called a proper mixing layer if no wall is invariant under $\lambda$.

We can characterize the translation-based class by the following:

Definition 2.2 ([2]). A block cipher $\mathcal{C} = \{ \tau_k \mid k \in \mathcal{K} \}$ over $\mathbb{F}_2$ is called translation based (tb) if:

- it is the composition of a finite number of rounds, such that any round $\tau_{k,h}$ can be written as $\gamma_h \lambda_h \sigma_{k,h}$, where
  - $\gamma_h$ is a round-dependent bricklayer transformation (but it does not depend on $k$) and $0 \gamma_h = 0$,
  - $\lambda_h$ is a round-dependent linear map (but it does not depend on $k$),
We denote with $L$ such that

\[ \text{formity to prevent differential cryptanalysis (see [2, Remark 3.3]).} \]

Let $m \geq 1$, and let $f : \mathbb{F}_2^m \rightarrow (\mathbb{F}_2)^m$ be a vectorial Boolean function. We denote by $\hat{f}_u(x) = f(x + u) + f(x)$ the derivative of $f$ in the direction of $u \in (\mathbb{F}_2)^m$.

**Definition 2.3.** Let $f$ be a vectorial Boolean function, for any $a, b \in (\mathbb{F}_2)^m$ we define

\[ \delta_f(a, b) = |\{ x \in (\mathbb{F}_2)^m \mid \hat{f}_u(x) = b \}|. \]

Then, $f$ is said differentially $\delta$-uniform if

\[ \delta = \max_{u \neq 0 \in (\mathbb{F}_2)^m} \delta_f(a, b). \]

Vectorial Boolean functions used as S-boxes in block ciphers must have low uniformity to prevent differential cryptanalysis (see [1]). By [2, Fact 3], a vectorial Boolean function differentially $\delta$-uniform satisfies

\[ |\text{Im}(\hat{f}_u)| \geq \frac{2^m}{\delta}. \]

**Definition 2.4.** Let $1 \leq r < m$ and $f(0) = 0$, we say that $f$ is strongly $r$-anti-invariant if, for any two subspaces $U$ and $W$ of $(\mathbb{F}_2)^m$ such that $f(U) = W$, then either $\dim(U) = \dim(W) < m - r$ or $U = W = (\mathbb{F}_2)^m$.

2.2. **Partition-based trapdoors.** We recall that a permutation group $G$ acting on $V$ is called called primitive if it has no nontrivial $G$-invariant partition of $V$. That is, there no exists a partition $A$ of $V$ different from the trivial partitions $\{\{v\} \mid v \in V\}$, $\{V\}$, such that $Ag \in A$ for all $A \in A$ and $g \in G$. On the other hand, if a nontrivial $G$-invariant partition exists, the group is called imprimitive.

As said before a property of $\Gamma_\infty$ considered undesirable is the imprimitivity. Paterson [9] showed that if this group is imprimitive, then it is possible to embed a trapdoor in the cipher.

Another trapdoor, based on the idea of the imprimitive action, is the Partition-based trapdoor, introduced in a recent work [11]. In this work the authors give some conditions to construct a translation-based cipher which associates a partition of the plaintext space to another partition of the ciphertext space.

We report some of the definitions and result presented in [11].

**Definition 2.5.** Let $\rho$ be a permutation of $V$ and $A, B$ be two partitions of $V$. Let $A \rho$ denote the set $\{ A \rho \mid A \in A \}$. We say that $\rho$ maps $A$ to $B$ if $A \rho = B$. Moreover, let $G$ be a permutation group we say that $G$ maps $A$ to $B$ if for all $\rho \in G$, $\rho$ maps $A$ to $B$.

**Remark 1.** Note that a permutation group $G$ is imprimitive if there exists a nontrivial partition $A$ such that for all $\rho \in G$, $A \rho = A$.

**Definition 2.6.** A partition $A$ of $V$ is said linear if there exists $U$ a subspace of $V$ such that

\[ A = \{ U + v \mid v \in V \}. \]

We denote with $L(U)$ such a partition.
The following result, introduced by Harpes in [12], characterizes the possible partitions \( A \) and \( B \) such that \( T(V) \) maps \( A \) to \( B \).

**Proposition 1.** Let \( A \) and \( B \) be two partitions of \( V = (\mathbb{F}_2)^d \). Then the permutation \( T(V) \) maps \( A \) to \( B \) if and only if \( A = B \) and \( A \) is a linear partition.

Focusing on the mixing-layer we have.

**Proposition 2 ([11]).** Let \( \lambda \) be a linear permutation of \( V \), i.e. \( \lambda \in \text{GL}(V) \), and let \( U \) be a subspace of \( V \). Then \( \mathcal{L}(U)\lambda = \mathcal{L}(U\lambda) \).

We report now the main theorem of [11]. In [11] the following result is reported for a SPN cipher with the same s-Box and mixing-layer for each round, but can be extended to any translation based cipher with independent round keys.

**Theorem 2.7.** Let \( C \) be a translation based cipher on \( V \). Suppose that there exist \( A \) and \( B \) non-trivial partitions such that for all \( \ell \)-tuples of round-keys \( k = (k_1, ..., k_\ell) \) the encryption function \( \tau_k \) maps \( A \) to \( B \). Define \( A_1 = A \) and for \( 1 \leq i \leq \ell \) \( A_{i+1} = A_i\tau_i \), where \( \tau_i = \gamma_i\lambda_i \) is the \( i \)-th round function without the round key translation. Then

- \( A_{\ell+1} = B \)
- for any \( 1 \leq i \leq \ell + 1 \) \( A_i \) is a linear partition.

3. Avoiding the partition-based trapdoor. In this section we will give sufficient conditions on the components of a tb cipher sufficient to guarantee that such a trapdoor cannot be implemented.

**Lemma 3.1.** Let \( \gamma \) be a permutation on \( V \) such that \( 0\gamma = 0 \) and suppose that \( \gamma \) maps \( \mathcal{L}(U) \) to \( \mathcal{L}(W) \) then for all \( u \in U \)

\[
\text{Im}(\hat{\gamma}_u) \subseteq W.
\]

**Proof.** The fact that \( \gamma \) maps \( \mathcal{L}(U) \) to \( \mathcal{L}(W) \) and \( 0\gamma = 0 \) imply that \( U\gamma = W \). Moreover for all \( v \in V \) we have that \( v\gamma \in (U + v)\gamma \). Then \( (U + v)\gamma = W + v\gamma \). This implies that

\[
(u + v)\gamma + v\gamma \in W
\]

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

From Lemma 3.1 we have the following.

**Proposition 3.** Let \( \gamma \) be a brick-layer transformation, i.e. \( \gamma = (\gamma_1, ..., \gamma_b) \) with \( \gamma_i \in \text{Sym}(V_i) \) for all \( i \). Suppose that for all \( i \gamma_i \) is

1. differentially \( 2^r \)-uniform, with \( r < m \),
2. strongly \((r-1)\)-anti-invariant

Let \( \mathcal{L}(U) \) and \( \mathcal{L}(W) \) be non-trivial linear partitions of \( V \), then \( \gamma \) maps \( \mathcal{L}(U) \) to \( \mathcal{L}(W) \) if and only if \( U \) and \( W \) are walls, in particular \( U = W \).

**Proof.** Suppose that \( \gamma \) maps \( \mathcal{L}(U) \) to \( \mathcal{L}(W) \) and that \( U \) is not a wall. Then let \( I = \{ i \mid \pi_i(U) \neq \emptyset \} \). There exists \( i \in I \) such that \( U \cap V_i \neq \emptyset \) because \( U \) is not a wall. Moreover \( U \cap V_i \neq \emptyset \). Indeed, let \( u \in U \), with \( u_i \neq 0 \). For all \( v \in V \) such \( v_j = 0 \) for all \( j \neq i \) we have that

\[
(u + v_i)\gamma + v_i\gamma \in W
\]

from Lemma 3.1. Moreover \( u\gamma \in W \). It follows that \( u\gamma + (u + v_i)\gamma + v_i\gamma \in W \). The vector \( u\gamma + (u + v_i)\gamma + v_i\gamma \) has all nonzero components but for the one in \( V_i \),
which is \( u_1 \gamma_i + (u_i + v_i) \gamma_i + v_i \gamma_i \in W \cap V_i \). As \( \gamma \) is a brick layer transformation, if \( U \cap V_i = \{0\} \), then \( W \cap V_i = \{0\} \). So, if the vector \( u_1 \gamma_i + (u_i + v_i) \gamma_i + v_i \gamma_i \) is zero for all \( v_i \in V_i \), then \( \text{Im}(\gamma_i) = \{u_i \gamma_i\} \), of size 1. This contradicts the first condition on the \( \gamma_i \)'s.

Thus \( U \cap V_i \) is a proper subspace of \( V_i \) and \((U \cap V_i) \gamma = W \cap V_i \) is also a proper subspace of \( V_i \). Being \( \text{Im}(\gamma_i) \subseteq W \) for all \( u \in U \), we have \( \text{Im}(\gamma_i) \subseteq W \cap V_i \) for all \( u \in U \cap V_i \). Thus, \( |\text{Im}(\gamma_i)| \) for any non-zero \( u \) is greater or equal to \( 2^{m-r} \) and, being \( \gamma_i \) a permutation, the set \( \text{Im}(\gamma_i) \) does not contain the zero vector, which implies \( \dim(W \cap V_i) \geq m - r + 1 \). This contradicts the second condition on the \( \gamma_i \)'s. Then, \( U \) is a wall and, being \( \gamma \) a parallel map \( U = W \).

Vice versa, consider any wall \( U \), as \( \gamma \) is a parallel map, it is easy to check that \( \gamma \) maps \( \{U + v \mid v \in V\} \) in itself.

The following definition was introduced in [10].

**Definition 3.2.** Let \( \lambda \in GL(V) \). \( \lambda \) is said to be a strongly proper mixing-layer if it does not map a proper wall in an other wall.

We define a strongly-proper round of a tb cipher as a proper round, where the mixing-layer is also strongly proper.

**Theorem 3.3.** Let a round \( h < \ell \) be a strongly proper round and suppose that the brick-layer transformations of round \( h \) and round \( h + 1 \), \( \gamma_h \) and \( \gamma_{h+1} \), satisfy Condition 1) and 2) of Proposition 3. Then, there do not exist \( A \) and \( B \) non-trivial partitions such that for all \( \ell \)-tuple of round keys the encryption functions map \( A \) to \( B \).

**Proof.** Suppose that the partition-based trapdoor is applicable for all \( \ell \)-tuple of round keys. From Theorem 2.7 we have that there exist two linear partitions \( L(U) \) and \( L(W) \) such that \( \gamma_h \lambda_h \) maps \( L(U) \) to \( L(W) \). Thus \( \gamma_h \lambda_h \) maps \( L(U) \) to \( L(W(\lambda_h)^{-1}) \).

From Proposition 3 we have that \( U \) is a wall and the same \( W(\lambda_h)^{-1} \).

Now being \( \lambda_h \) strongly-proper we have that \( W \) is not a wall. Then from Theorem 2.7 we have that \( \gamma_{h+1} \lambda_{h+1} \) maps \( L(W) \) to another linear partition, but it is not possible as \( W \) is not a wall and this contradicts Proposition 3.

The result of Theorem 3.3 can be generalized, using a weaker condition on the mixing-layers composing the round functions. Consider, for example, the mixing-layer of AES. This is not strongly-proper, as there exists a wall which is sent in another wall. Indeed, the state of AES can be represented as a \( 4 \times 4 \) matrix of bytes (Table 1). That is, \( V = V_1 \oplus ... \oplus V_{16} \), where \( V_i \) is isomorphic to \((F_2)^8\).

| \( V_0 \) | \( V_1 \) | \( V_2 \) | \( V_3 \) | \( V_4 \) | \( V_5 \) | \( V_6 \) | \( V_7 \) | \( V_8 \) | \( V_9 \) | \( V_{10} \) | \( V_{11} \) | \( V_{12} \) | \( V_{13} \) | \( V_{14} \) | \( V_{15} \) | \( V_{16} \) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| \( V_0 \) | \( V_1 \) | \( V_2 \) | \( V_3 \) | \( V_4 \) | \( V_5 \) | \( V_6 \) | \( V_7 \) | \( V_8 \) | \( V_9 \) | \( V_{10} \) | \( V_{11} \) | \( V_{12} \) | \( V_{13} \) | \( V_{14} \) | \( V_{15} \) | \( V_{16} \) |

**Table 1.** AES state

The mixing-layer of AES is composed by two linear functions ShiftRow (SR) and MixColumn (MC). The ShiftRows transformation acts in a way such that a wall is sent in an other wall, and in particular \( V_1 \oplus V_6 \oplus V_{11} \oplus V_{16} \) is sent in \( V_1 \oplus V_5 \oplus V_9 \oplus V_{13} \).

Now, as MixColumn combines the blocks of a same column of the state, we have that \( V_1 \oplus V_5 \oplus V_9 \oplus V_{13} \) (which is the first column of the state) is sent in itself (Table 2). However, the previous attack cannot be applied to AES as the mixing layer satisfies the following property.
Definition 3.4. Let \( \lambda_1, \ldots, \lambda_\ell \) be the mixing-layers used in a tb cipher with \( \ell \) rounds. We say that the ordered family \( \Lambda = (\lambda_1, \ldots, \lambda_\ell) \) is strongly proper if for all possible non-trivial wall \( W \) there exists \( j < \ell \) such that \( W \lambda_1 \cdot \ldots \cdot \lambda_j \) is not a wall.

Corollary 1. Let \( C \) be a tb cipher with \( \Lambda = (\lambda_1, \ldots, \lambda_\ell) \) strongly proper and for each round \( h \) the parallel map \( \gamma_h \) satisfies the conditions of Proposition 3. Then the partition-based trapdoor is not applicable.

Proof. Suppose that the partition-based trapdoor is applicable. From Theorem 2.7 we have that each round functions (without the translation with respect to the round key) \( \tau_h = \gamma_h \lambda_h \) maps a linear partition \( \mathcal{L}(U_h) \) into \( \mathcal{L}(U_{h+1}) \). From Lemma 3.1 the space \( U_h \) is a wall for all \( 1 \leq h \leq \ell \). Then, being \( \gamma_h \) a parallel map and \( 0 \gamma_h = 0 \) we have

\[
U_{h+1} = U_h \lambda_h = U_1 \lambda_1 \cdot \ldots \cdot \lambda_h
\]

for all \( h \).

Since \( \Lambda \) is strongly proper, there exists \( j < \ell \) such that \( U_1 \lambda_1 \cdot \ldots \cdot \lambda_j \) is not a wall, which contradicts the fact that \( U_h \) is a wall for all \( 1 \leq h \leq \ell \).

It may seem that the previous corollary requires strong conditions on the mixing layers and on the S-boxes. We show that the requirement on the mixing layers is necessary.

Proposition 4. Let \( C \) be a tb cipher, with \( \Lambda = (\lambda_1, \ldots, \lambda_\ell) \) not strongly proper. Then the partition trapdoor is applicable.

Proof. Because \( \Lambda = (\lambda_1, \ldots, \lambda_\ell) \) is not strongly proper, then there exists \( W \) a proper wall such that \( W \lambda_1 \cdot \ldots \cdot \lambda_j \) is a wall for all \( 1 \leq j \leq \ell \). Now being the \( \gamma_h \) a parallel map we have that for all wall \( W' \) and \( v \in V \)

\[
(W' + v) \gamma_h = W' + v \gamma_h,
\]

which concludes the proof.

4. Security proof for a cipher with independent round-keys. In this section we will discuss the fact that studying the group \( \Gamma_\infty \) to understand the security of a block cipher \( C \) could not be enough.

We report an example of block cipher \( C \) whose components satisfy the cryptographic properties given in [10] sufficient to thwart the trapdoor introduced by Paterson [9], but that is weak with respect to the partition-based trapdoor.

Let \( V = (\mathbb{F}_2)^{mb} \), \( V_i = (\mathbb{F}_2)^{m} \), with \( m, b \geq 1 \) and \( \gamma_i \in \text{Sym}(V_i) \) be the inverse permutation for all \( 0 \leq i \leq b - 1 \), i.e. \( \gamma_i : x \mapsto x^{2^m-2} \) (using the representation as
univariate polynomial). Consider the following mixing-layer

\[
\lambda = \begin{bmatrix}
0 & I_{m \times m} & 0 & \ldots & 0 \\
0 & 0 & I_{m \times m} & \ldots & 0 \\
\vdots & \vdots & & \ddots & \vdots \\
0 & \ldots & & I_{m \times m} & 0 \\
I_{m \times m} & \ldots & & & 0 \\
\end{bmatrix}
\]

where \( I_{m \times m} \) is the identity matrix of size \( m \times m \). It is easy to check that \( \lambda \) is a proper mixing-layer but not strongly proper.

Consider now the linear partitions \( \mathcal{L}(V_1), \ldots, \mathcal{L}(V_b) \), and suppose to have \( \ell \) rounds where we use \( \lambda \) and \( \gamma \) in each one. From [10, Theorem 3.1] \( \Gamma_\infty(C) \) is primitive, but each encryption function maps \( \mathcal{L}(V_i) \) to \( \mathcal{L}(V_{\sigma(i)}) \), where \( \sigma \) is the permutation of \( \{1, \ldots, b\} \) such that \( \sigma : i \mapsto i + 1 \) for all \( i < b \) and \( \sigma : b \mapsto 1 \).

Obviously, the mixing-layer \( \lambda \) is not interesting from a cryptographic point of view.

We use this only as an example to show that if \( \Gamma_\infty(C) \) is primitive this does not guarantee security on \( C \). Moreover, if we use a number \( \ell \) of rounds such that \( \mathcal{L}(V_i) = \mathcal{L}(V_{\sigma(i)}) \) for some \( i \), then \( \Gamma_\infty(C) \) is primitive and the group \( \Gamma(C) \) is imprimitive.

As we pointed out in Section 2, it would be interesting to study the group \( \Gamma(C) \).

However, this group depends, strongly, on the key-schedule used to create the round-keys. For this reason, usually, we study the properties of the group \( \Gamma_\infty(C) \). But, as we showed above, we could have that even if the group \( \Gamma_\infty(C) \) is consider secure, the group \( \Gamma(C) \) may be not secure with respect to the trapdoors considered here.

Then, we think that it is better to consider, and study, the group of a cipher \( C \) obtained using independent round-keys, that is,

\[
\Gamma_{ind}(C) = \langle \tau_K \mid K \in V^{\ell} \rangle,
\]

where, letting \( K = (k_1, \ldots, k_\ell) \), \( \tau_K \) is the encryption function obtained using \( k_h \in V \) as round-key at round \( h \). Clearly, \( \Gamma_{ind}(C) \) is such that

\[
\Gamma(C) \subseteq \Gamma_{ind}(C) \subseteq \Gamma_\infty(C).
\]

We can summarize the results obtained in this work for \( \Gamma_{ind}(C) \) in the following:

**Theorem 4.1.** Let \( C \) be a tb cipher. Suppose that one of the following properties is satisfied:

1. there exists a round \( h \) which is a strongly proper round and the brick-layer transformations \( \gamma_h, \gamma_{h+1} \) satisfy Condition 1) and 2) of Proposition 3,

or

2. the family \( \Lambda = (\lambda_1, \ldots, \lambda_\ell) \) is strongly proper and for each round \( h \) the parallel map \( \gamma_h \) satisfies Condition 1) and 2) of Proposition 3.

Then the partition-based trapdoor is not applicable. Moreover, \( \Gamma_{ind}(C) \) is primitive.

**Proof.** From Theorem 3.3 (or Corollary 1) we have that there do not exist two partitions \( A \) and \( B \) such that \( A_{\tau_k} = B \) for all \( \tau_k \in \Gamma_{ind}(C) \). Moreover, the group \( \Gamma_{ind}(C) \) is imprimitive if and only if there exists a partition such that \( A_{\tau_k} = A \) for all \( \tau_k \in \Gamma_{ind}(C) \) (see Remark 1), which is a particular case where the partition-based trapdoor is applicable.

5. **Conclusions.** An interesting open problem proposed by Paterson [9] is to investigate if it is possible to construct a block cipher such that the group \( \Gamma_\infty \) is primitive, but the resulting cipher is weak with respect to the imprimitive trapdoor. As we pointed out in Section 4, it may happen that the cipher is vulnerable.
even if the group generated by the round functions results to be primitive. For this reason, here, we studied the group \( \Gamma_{\text{ind}} \) generated by the cipher with independent round keys. We think that studying algebraic properties for this group could be more appropriate to investigate security properties of a cipher. In particular, we gave sufficient conditions on the components of a cipher \( C \), so that the partition trapdoor given in [11] cannot be applied to the encryption functions generating \( \Gamma_{\text{ind}}(C) \). As a consequence, we obtained also the primitivity for the group \( \Gamma_{\text{ind}}(C) \).

Note that this type of trapdoor can be easily avoided. Indeed, as noted in [10], for an invertible vectorial Boolean function to be strongly 1-anti-invariant is equivalent to have no linear components (i.e. the nonlinearity is greater than 0). Such a property is usually requested by the S-boxes of a cipher to avoid linear cryptanalysis. Moreover, to achieve a good diffusion we need that the mixing layer satisfies the condition given in Definition 3.4. Therefore, from Theorem 4.1, sufficient conditions to thwart the partition trapdoor are:

- S-boxes with differential 4-uniformity and nonlinearity different from 0.
- strongly proper mixing layers (or that satisfy the condition in Definition 3.4).

Another requested property for a cipher is that the group generated by the encryption functions is not “small” (see for instance [8]). Usually, this property is investigated for the group of the round functions ([13, 14]). In [3, 10] are given conditions for tb ciphers so that \( \Gamma_{\infty} \) is the symmetric (alternating) group.

In the case of ciphers like AES, where the same S-box and mixing layer are used in each round, we have that \( \Gamma_{\text{ind}}(C) \) is normal in \( \Gamma_{\infty}(C) \), so if \( \Gamma_{\infty}(C) \) is the symmetric (alternating) group we have the same for \( \Gamma_{\text{ind}}(C) \). However, this is no more the case of ciphers like, e.g., SERPENT, where the used S-box depends on the round. Then, it may happen that the group of the round functions generates the symmetric (alternating) group, while the group generated by the encryption functions is not. An interesting future research could be investigating assumptions on the components of a cipher \( C \) which can guarantee that the group \( \Gamma_{\text{ind}}(C) \) is the symmetric (alternating) group.

References

[1] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. Journal of CRYPTOLOGY, 4(1):3–72, 1991.
[2] A. Caranti, F. Dalla Volta, M. Sala, On some block ciphers and imprimitive groups, AAECC 20 (5-6), 229–350, 2009.
[3] 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 (2009): 293-301.
[4] J. Daemen, V. Rijmen. The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2002.
[5] R. Anderson, E. Biham, L. Knudsen, SERPENT: A New Block Cipher Proposal, in: Fast Software Encryption, Vol. 1372 of LNCS, Springer, pp. 222–238, 1998.
[6] A. Andrey Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher, in: Proc. of CHES 2007, Vol. 4727 of LNCS, Springer, pp. 450–466, 2007.
[7] D. Coppersmith, E. Grossman. Generators for certain alternating groups with applications to cryptography. SIAM Journal on Applied Mathematics 29 (4), 624–627, 1975.
[8] Kaliski, Burton S., Ronald L. Rivest, and Alan T. Sherman. Is the Data Encryption Standard a group? Results of cycling experiments on DES. Journal of Cryptology 1.1: 3–36, 1988.
[9] K. G. Paterson. Imprimitive permutation groups and trapdoors in iterated block ciphers, in: Fast Software Encryption, Vol. 1636 of LNCS, Springer, Berlin, pp. 201–214, 1999.
[10] R. Aragona, M. Calderini, A. Tortora, M. Tota, *On the primitivity of PRESENT and other lightweight ciphers*. arXiv preprint arXiv:1611.01346, 2016.
[11] A. Bannier, N. Bodin, E. Filiol, *Partition-Based Trapdoor Ciphers*. Cryptology ePrint Archive, Report 2016/493, 2016.
[12] C. Harpes, J. L. Massey, *Partitioning cryptanalysis*, in: Fast Software Encryption, Springer, pp. 13–27, 1997.
[13] S. Even and O. Goldreich, *DES-Like functions can generate the alternating group*. IEEE Trans. Inform. Theory, 863–865, 1983.
[14] R. Sparr and R. Wernsdorf, *Group theoretic properties of Rijndael-like ciphers*. Discrete Appl. Math. 156, no. 16, 3139–3149, 2008.

Received xxxx 20xx; revised xxxx 20xx.

E-mail address: marco.calderini@unitn.it