

Manuscript submitted to  
AIMS' Journals  
Volume **X**, Number **0X**, XX **200X**

doi:10.3934/xx.xx.xx.xx

pp. **X–XX**

## SOME GROUP-THEORETICAL RESULTS ON FEISTEL NETWORKS IN A LONG-KEY SCENARIO

RICCARDO ARAGONA\*

DISIM, University of L'Aquila  
Via Vetoio, 67100 Coppito (AQ), Italy

MARCO CALDERINI

Department of Informatics, University of Bergen  
Postboks 7803, N-5020 Bergen, Norway

ROBERTO CIVINO

DISIM, University of L'Aquila  
Via Vetoio, 67100 Coppito (AQ), Italy

(Communicated by the associate editor name)

**ABSTRACT.** The study of the trapdoors that can be hidden in a block cipher is and has always been a high-interest topic in symmetric cryptography. In this paper we focus on Feistel-network-like ciphers in a classical long-key scenario and we investigate some conditions which make such a construction immune to the partition-based attack introduced recently by Banner et al.

**1. Introduction.** Most modern block ciphers belong to two families of symmetric cryptosystems, i.e. Substitution-Permutation Networks (SPN) and Feistel Networks. Typically, in both cases, each encryption function is a composition of key-dependent permutations of the plaintext space, called *round functions*, designed in a such way to provide both *confusion* and *diffusion* (see [21]). Confusion is provided applying public non-linear vectorial Boolean functions, called S-boxes, whereas diffusion is obtained by means of public linear maps, called diffusion layers. The private component of the cipher, i.e. the *key*, is derived from the user-provided information by means of a public procedure known as *key-schedule*. When the round functions are made in such a way the confusion and diffusion layers are followed by the XOR-addition with the so-called *round-key*, where the round-key is every possible vector in the message space, the cipher is a *long-key cipher*.

Since the seventies, many researchers have studied the relationship between some algebraic properties of the confusion / diffusion layers and some algebraic weaknesses of the corresponding ciphers, using a permutation-group-theoretical approach. In 1975, Coppersmith and Grossman [13] considered a set of permutations

---

2010 *Mathematics Subject Classification.* Primary: 94A60, 20B05; Secondary: 20B35.

*Key words and phrases.* Symmetric Cryptography, Block Cipher, Trapdoor, Group Generated by Round Functions, Partitions.

All the authors are members of INdAM-GNSAGA (Italy). Part of this work was carried out during Marco Calderini's visit at University of LAquila, supported by the Meltzer Research Fund and Trond Mohn Foundation.

\* Corresponding author: xxxx.

which can be used to define a block cipher and, by studying the permutation group that they generate, they linked some properties of this group and the security of the corresponding cipher. From this work a new branch of research was born, which focuses on group-theoretical properties that can be exploited to attack encryption methods. In [18], the authors proved that if the permutation group generated by the encryption functions of a cipher is too small, then the cipher is vulnerable to birthday-paradox attacks. In [10] the authors proved that if such group is isomorphic to a subgroup of the affine group of the plaintext space, induced by a sum different to the classical bitwise XOR, then it is possible to embed a dangerous trapdoor on it. More relevant in [19], Paterson built a DES-like [15] cipher whose encryption functions generate an imprimitive group and showed how the knowledge of this trapdoor can be turned into an efficient attack to the cipher. For this reason, showing that the group generated by the encryption functions of a given cipher is primitive and not of affine type became a relevant branch of research (see [2, 3, 4, 11, 12, 22, 23, 24, 25]). Recently, in [5, 6] the imprimitive attack shown by Paterson was generalized by means of a trapdoor which consists in mapping a partition of the plaintext space into a (different) partition of the ciphertext space. The authors also proved that only *linear* partitions can propagate round-by-round in a long-key SPN. Later Calderini [9] has shown which conditions ensure that linear partitions cannot propagate in a long-key SPN.

In this work we study some properties of the linear-partition propagation under the action of a long-key Feistel network. In particular, our aim is to prove that also in a Feistel-network-like long-key framework, if the cipher allows partition propagation, then the partitions are linear one. Moreover, we provide a partial generalisation of Calderini's result in the Feistel network case.

**2. Preliminaries and notation.** The notation and parameters which are used throughout this paper are presented in the following section.

Let  $n \in \mathbb{N}$  and let us denote  $V = (\mathbb{F}_2)^n$  the  $n$ -dimensional vector space over  $\mathbb{F}_2$  equipped with the bit-wise XOR. Let us suppose  $\dim(V) = n = bs$  and let us write  $V = V_1 \oplus V_2 \oplus \dots \oplus V_b$  where for  $1 \leq j \leq b$ ,  $\dim(V_j) = s$  and  $\oplus$  represents the direct sum of vector subspaces. The subspaces  $V_j$  are called *bricks*. For any  $I \subset \{1, \dots, b\}$ , with  $I \neq \emptyset$  and  $I \neq \{1, \dots, b\}$ , the direct sum  $\bigoplus_{i \in I} V_i$  is called a *wall*. We denote by  $\text{Sym}(V)$  the symmetric group acting on  $V$ , i.e. the group of all the permutations on  $V$ . Let us also denote by  $\text{AGL}(V)$  the group of all affine permutations of  $V$ , which is a primitive maximal subgroup of  $\text{Sym}(V)$ . The translation group on  $V$  is denoted by  $T(V)$ , i.e.  $T(V) \stackrel{\text{def}}{=} \{\sigma_v \mid v \in V, x \mapsto x + v\} < \text{Sym}(V)$ .

Let us now introduce block ciphers, the subject of this work.

**2.1. Block ciphers.** Let  $\mathbb{M}$  and  $\mathbb{K}$  be non-empty sets, where  $|\mathbb{K}| \geq |\mathbb{M}|$ . A *block cipher*  $\Phi$  is a family of key-dependent permutations

$$\{E_K \mid E_K : \mathbb{M} \rightarrow \mathbb{M}, K \in \mathbb{K}\},$$

where  $\mathbb{M}$  is called the message space and  $\mathbb{K}$  the key space. The permutation  $E_K$  is called the *encryption function induced by the master key  $K$* . The block cipher  $\Phi$  is called an *iterated block cipher* if there exists  $r \in \mathbb{N}$  such that for each  $K \in \mathbb{K}$  the encryption function  $E_K$  is the composition of  $r$  key-dependent *round functions*, i.e.

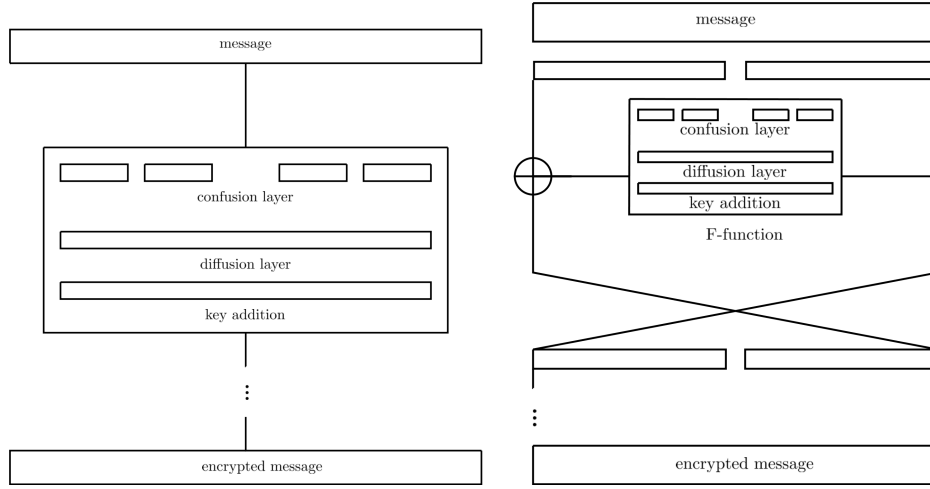


FIGURE 1. Round function of an SPN and of a Feistel network

$E_K = \varepsilon_{1,K} \varepsilon_{2,K} \dots \varepsilon_{r,K}$ . To provide efficiency, each round function is the composition of a public component provided by the designers, and a private component derived from the user-provided key by means of a public procedure known as *key-schedule*.

In the theory of modern iterated block cipher, two frameworks are mainly considered: Substitution-Permutation Networks, typically abbreviated as SPN (see e.g. AES [14]) and Feistel networks (see e.g. [15]). Figure 1 depicts the more general framework of SPNs, Feistel networks and their round functions; notice that inside the round function of a Feistel network, a function called F-function is applied to a half of the state. In both cases, the principles of confusion and diffusion suggested by Shannon [21] are implemented by considering each round function (or respectively F-function) as the composition of key-induced permutation as well as non-linear confusion layers and linear diffusion layers, which are invertible in the case of SPNs and preferably (but not necessarily) invertible in the case of Feistel networks. The following definition has been given in [1] and introduces a class of round functions for iterated block ciphers which is large enough to include the round functions of well-established SPNs and some F-functions of Feistel networks.

**Definition 2.1.** A *classical round function* is a map of the type  $\varepsilon_k = \gamma\lambda\sigma_k \in \text{Sym}(V)$ , where  $k \in V$  and

- $\gamma : V \rightarrow V$  is a non-linear permutation (parallel S-box) which acts in parallel way on each  $V_j$ , i.e.

$$(x_1, x_2, \dots, x_n)\gamma = \left( (x_1, \dots, x_s)\gamma^{(1)}, \dots, (x_{s(b-1)+1}, \dots, x_n)\gamma^{(b)} \right).$$

The maps  $\gamma^{(j)} : V_j \rightarrow V_j$  are traditionally called S-boxes;

- $\lambda \in \text{Sym}(V)$  is a linear map, called *diffusion layer*;
- $\sigma_k : V \rightarrow V, x \mapsto x + k$ , called *key-addition* layer, represents the addition with the round key  $k$ , where  $+$  is the usual bitwise XOR.

In modern literature, terms *SPN* (or the similar notion of *translation-based cipher* [11]) and *Feistel network* may refer to a very diverse variety of ciphers. For the purposes of this paper we choose to focus only on ciphers with an XOR-based key addition. For this reason, saying SPN we refer to any cipher  $\{E_K \mid K \in \mathbb{K}\} \subseteq \text{Sym}(\mathbb{M})$  having an SPN-like structure with  $\mathbb{M} = V$  and having classical round functions on  $V$  as round functions, and saying Feistel network to any cipher  $\{E_K \mid K \in \mathbb{K}\} \subseteq \text{Sym}(\mathbb{M})$  having a Feistel-network-like structure with  $\mathbb{M} = V \times V$  and having classical round functions on  $V$  as F-functions. In both cases, the composition  $\rho_i \stackrel{\text{def}}{=} \gamma_i \lambda_i$  is called the *generating function* of the  $i$ -th round of the cipher. Notice that usually in real-life ciphers it holds  $\rho_1 = id_V$ , which means that in the first round only a key addition is applied to the plaintext (*whitening*). In this setting, an  $r$ -round cipher is defined once the list of its generating functions  $\rho_1, \dots, \rho_r$  and its key-schedule are given.

Once the key  $K \in \mathbb{K}$  to be used for the encryption has been chosen, the encryption function is obtained by composing the  $r$  classical round functions induced by the corresponding round keys, which are, as previously mentioned, derived by the key-schedule. Hence, in the quite popular setting in which the round key is XORed to the state, the key-schedule is a function

$$\mathcal{S} : \mathbb{K} \rightarrow V^r$$

such that  $\mathcal{S}(K) \stackrel{\text{def}}{=} (k_1, \dots, k_r)$  for any  $K \in \mathbb{K}$ , where  $\mathcal{S}(K)_i \stackrel{\text{def}}{=} k_i$  is the  $i$ -th round key derived from the user-provided key  $K$  and  $\varepsilon_{i,K} = \varepsilon_{\mathcal{S}(K)_i}$ .

In the following section we recall some basic security notion for Boolean function that we will use later.

**2.2. Security notions for Boolean functions.** The following property is the standard request for the linear component of a block cipher to spread the input bits as much as possible within the ciphertext.

**Definition 2.2.** A linear map  $\lambda \in \text{GL}(V)$  is called a *proper diffusion layer* if no wall is invariant under  $\lambda$  and it is called a *strongly proper diffusion layer* if there are no walls  $W$  and  $W'$  such that  $W\lambda = W'$ .

In the remainder of this section we recall notions of non-linearity which will be useful in this work. Let us recall that the non-linear layer of the ciphers which will be considered throughout this work act applying vectorial Boolean functions  $\gamma^{(i)}$  to each brick of the block. Notice that we can always assume  $0\gamma^{(i)} = 0$  without loss of generality, since otherwise  $0\gamma^{(i)}$  can be included as part of key-addition layer of the previous round, for each round index  $1 \leq i \leq b$  (see [11, Remark 3.3]).

**Definition 2.3.** Let  $f \in \text{Sym}((\mathbb{F}_2)^s)$ . Let us define

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

The map  $f$  is said  $\delta$ -differentially uniform if

$$\delta = \max_{\substack{a, b \\ a \neq 0}} \delta_f(a, b).$$

It is known that  $\delta$ -differentially uniform functions with small  $\delta$  are “farther” from being linear compared to functions with a larger differential uniformity. Notice

indeed that when  $f$  is linear, then  $\delta = 2^s$ . Let us recall that 2-differentially uniform S-boxes, which reach the lower bound of the previous definition, are called *Almost Perfect Non-linear (APN)*. Vectorial Boolean functions used as S-boxes in block ciphers must have low uniformity to prevent differential cryptanalysis (see [7]) and so APN S-boxes usually represent an optimal choice in terms of resistance to differential attacks.

We conclude this section giving another notion of non-linearity that we will use in some results of this work.

**Definition 2.4** ([11]). Let  $1 \leq \delta < s$  and  $f \in \text{Sym}((\mathbb{F}_2)^s)$  such that  $f(0) = 0$ . The function  $f$  is *strongly  $\delta$ -anti-invariant* if for each  $U$  and  $W$  proper and non-trivial subspaces of  $(\mathbb{F}_2)^s$ , then

$$Uf = W \implies \dim(U) = \dim(W) < s - \delta.$$

Notice that if  $1 \leq \delta < \delta' < s$  and  $f$  is strongly  $\delta'$ -anti-invariant, then it is also strongly  $\delta$ -anti-invariant.

**2.3. A long-key scenario.** As mentioned in the introduction, the focus of this work is on a specific type of key-schedule, i.e. the one defined as follows:

**Definition 2.5.** Let  $\Phi$  be an  $r$ -round cipher on  $\mathbb{M}$  and let  $\mathcal{S} : \mathbb{K} \rightarrow V^r$  its key-schedule. Then  $\Phi$  is called a *long-key cipher* if  $\mathcal{S}(\mathbb{K}) = V^r$ .

The group generated by the encryption functions of a long-key cipher and its properties will be investigated throughout this work. In the next section we will, in particular, study its behavior in relation to the attacks described in the following section.

**3. Group-theoretical trapdoors.** The study of groups related to block ciphers may reveal weaknesses which can be exploited to perform algebraic attacks. In this paper, we focus on some particular group-theoretical attacks (see e.g. [19, 5]), based on undesirable properties of such permutation groups. Notice that the study of the group generated by the encryption functions is a hard task in general, since the dependence on the key-schedule is not easily turned into algebraic conditions. The aim of this work is to study the group generated by the encryption functions of  $\Phi$ , denoted by  $\Gamma(\Phi)$ , in an easier setting, i.e. the one of a long-key cipher. In particular we will focus on Feistel networks, providing a first generalisation of the results obtained in [9] regarding translation-based ciphers. For this purpose we also make use of the following group

$$\Gamma_h(\Phi) \stackrel{\text{def}}{=} \langle \varepsilon_{h,K} \mid K \in \mathbb{K} \rangle,$$

where all the possible round keys for round  $h$  are considered. From this, the group

$$\Gamma_\infty(\Phi) \stackrel{\text{def}}{=} \langle \Gamma_h(\Phi) \mid 1 \leq h \leq r \rangle.$$

can be obtained. As mentioned in Section 1, the group  $\Gamma_\infty$  has been extensively studied in recent years, being the closest to the one generated by the encryption function that can be successfully investigated. However it is worth stressing that  $\Gamma_\infty(\Phi)$  may be *a-priori* way larger than the actual group of the encryption functions  $\Gamma(\Phi)$ .

The *imprimitivity* of such a group is one of the properties which may easily lead an attacker to a successful break of the cipher. The imprimitivity attack and its generalisation are described in the following section.

**3.1. Imprimitive action and partition-based trapdoor.** We recall that a permutation group  $G$  acting on  $V$  is called *primitive* if no non-trivial partition of  $V$  is invariant under the action of  $G$ , i.e. there is no partition  $\mathcal{A}$  of  $V$ , different from the trivial partitions  $\{\{v\} \mid v \in V\}$  and  $\{V\}$ , such that  $Ag \in \mathcal{A}$  for all  $A \in \mathcal{A}$  and  $g \in G$ . On the other hand, if a non-trivial  $G$ -invariant partition  $\mathcal{A}$  exists, the group is called *imprimitive*. Each  $A \in \mathcal{A}$  is called an *imprimitivity block*.

The imprimitivity is a very undesirable property for group generated by the encryption functions of a block cipher. As Paterson [19] showed, indeed, if this group is imprimitive, then it is possible to embed a trapdoor in the cipher which may allow attackers to recover crucial key-information with way less effort than a bruce force attack. Moreover, in [11] the authors characterised the cryptographic conditions of the boolean components of a cipher which guarantee that the corresponding group  $\Gamma_\infty$  is primitive. These results apply to the family of translation-based ciphers (see [11]), which is large enough to contain some of the most popular encryption methods (see [8, 14]). The conditions on the layers of the cipher which will be considered in this work are the same used in [11], or generalisation of those. The idea of attacking a cipher by exploiting the imprimitive action of its group has been generalized in a recent work [5], where the partition-based attack is introduced. The basic idea behind the attack is that, even if the group is primitive, it may exists a sequence of partitions  $\mathcal{A}_1, \dots, \mathcal{A}_r$  such that the  $i$ -th round function of each encryption function maps  $\mathcal{A}_i$  into  $\mathcal{A}_{i+1}$ . It is not hard to notice that, provided that this condition is true, the cipher can be attacked using an argument similar to the one exploiting the imprimitivity. In [5], the authors show an example of such attack on an SPN.

We report here some of the definitions and results presented in [5].

**Definition 3.1.** Let  $\rho \in \text{Sym}(V)$  and  $\mathcal{A}, \mathcal{B}$  be two partitions of  $V$ . Let  $\mathcal{A}\rho$  denote the set  $\{\mathcal{A}\rho \mid A \in \mathcal{A}\}$ . We say that  $\rho$  maps  $\mathcal{A}$  into  $\mathcal{B}$  if  $\mathcal{A}\rho = \mathcal{B}$ . Moreover, if  $G$  is a permutation group we say that  $G$  maps  $\mathcal{A}$  into  $\mathcal{B}$  if for all  $\rho \in G$ ,  $\rho$  maps  $\mathcal{A}$  into  $\mathcal{B}$ .

**Definition 3.2.** A partition  $\mathcal{A}$  of  $V$  is called *linear* if there exists  $U < V$  such that

$$\mathcal{A} = \{U + v \mid v \in V\}.$$

We denote  $\mathcal{A}$  by  $\mathcal{L}(U)$ .

The following result, introduced by Harpes and Massey in [17], characterizes the possible partitions  $\mathcal{A}$  and  $\mathcal{B}$  such that the translation group  $T(V)$  maps  $\mathcal{A}$  into  $\mathcal{B}$ .

**Proposition 1.** *Let  $\mathcal{A}$  and  $\mathcal{B}$  be two partitions of  $V$ . Then  $T(V)$  maps  $\mathcal{A}$  into  $\mathcal{B}$  if and only if  $\mathcal{A} = \mathcal{B}$  and  $\mathcal{A}$  is a linear partition.*

We report now the main result of [5].

**Theorem 3.3.** *Let  $\Phi$  be an  $r$ -round long-key SPN on  $\mathbb{M} = V$ . Suppose that there exist non-trivial partitions  $\mathcal{A}$  and  $\mathcal{B}$  such that for each key  $K$  the encryption function  $E_K$  maps  $\mathcal{A}$  to  $\mathcal{B}$ . Define  $\mathcal{A}_1 = \mathcal{A}$  and  $\mathcal{A}_{i+1} = \mathcal{A}_i \rho_i$  for  $1 \leq i \leq r$ , where  $\rho_i$  is the classical round function for the  $i$ -th round. Assume also that  $\rho_1$  is the identity map. Then*

- $\mathcal{A}_{r+1} = \mathcal{B}$
- $\mathcal{A}_i$  is a linear partition for any  $1 \leq i \leq r + 1$ .

In the previously shown result, Banner et al. proved that the only partitions which propagate round-by-round are the linear ones. The next results, proved in [9], shows which conditions are sufficient to avoid the linear-partition propagation in the SPN case. The aim of this work is to provide a partial generalisation of these results in the Feistel network case.

**Proposition 2.** *Let  $\gamma \in \text{Sym}(V)$  be a parallel S-box, i.e.  $\gamma = (\gamma^{(1)}, \dots, \gamma^{(b)})$  with  $\gamma^{(i)} \in \text{Sym}(V_i)$  for all  $1 \leq i \leq b$ . Suppose that for all  $1 \leq i \leq b$  the function  $\gamma^{(i)}$  is*

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

*Let  $\mathcal{L}(U)$  and  $\mathcal{L}(W)$  be non-trivial linear partitions of  $V$ . Then  $\gamma$  maps  $\mathcal{L}(U)$  into  $\mathcal{L}(W)$  if and only if  $U$  and  $W$  are wall. Moreover  $U = W$ .*

As a consequence, Calderini derived the following result, which guarantees immunity from the partition-based attack [9].

**Theorem 3.4.** *Let  $\rho_1, \dots, \rho_r \in \text{Sym}(V)$  and let  $\Phi$  be an  $r$ -round SPN on  $\mathbb{M} = V$ , where the  $i$ -th round applies  $\rho_i = \gamma_i \lambda_i$  such that  $0\rho_i = 0$ . Let us assume that for some  $1 \leq i < r$  we have*

- $\gamma_i$  and  $\gamma_{i+1}$  are parallel maps which apply  $2^\delta$ -differentially uniform and  $(\delta - 1)$ -strongly anti-invariant S-boxes, for some  $\delta < m$ ,
- $\lambda_i$  a strongly-proper diffusion layer.

*Then no encryption function  $E_K$  maps a non-trivial partition of  $V$  into a non-trivial partition of  $V$ .*

**4. Results.** As previously mentioned, the aim of this work is to prove, for long-key Feistel networks, some results which are linked to those recalled in the previous section. We study the linear partition-propagation under the action of a long-key Feistel network. The results obtained may be considered as a starting-point for a complete generalisation of the the results of Sect. 3.1 to Feistel networks, proved in [9] for translation-based ciphers. For this purpose, let us consider a typical Feistel structure. Let us introduce a formal  $2n \times 2n$  matrix which implements the Feistel structure. Such a formal matrix is defined as

$$\bar{\rho} \stackrel{\text{def}}{=} \begin{pmatrix} 0_n & 1_n \\ 1_n & \rho \end{pmatrix},$$

where  $0_n$  in the  $n \times n$  zero matrix,  $1_n$  is the  $n \times n$  identity matrix and  $\bar{\rho}$  is called *Feistel operator induced by the generating function  $\rho$* , whose right action on  $(x_1, x_2) \in V \times V$  is given by

$$(x_1, x_2)\bar{\rho} = (x_1, x_2) \begin{pmatrix} 0_n & 1_n \\ 1_n & \rho \end{pmatrix} \stackrel{\text{def}}{=} (x_2, x_1 + x_2\rho).$$

Note that  $\bar{\rho}$  has the inverse matrix

$$\bar{\rho}^{-1} \stackrel{\text{def}}{=} \begin{pmatrix} \rho & 1_n \\ 1_n & 0_n \end{pmatrix}.$$

Let us define

$$\begin{aligned} \sigma_{(h,k)} : V \times V &\rightarrow V \times V \\ (x_1, x_2) &\mapsto (x_1 + k, x_2 + h), \end{aligned}$$

and

$$T(V \times V) \stackrel{\text{def}}{=} \{\sigma_{(h,k)} \mid (h,k) \in V \times V\}.$$

Let  $\Phi$  be an  $r$ -round long-key Feistel network acting on  $V \times V$ , having the following  $i$ -th round function

$$\varepsilon_{i,K} = \bar{\rho}_i \sigma_{(0,k_i)},$$

where  $\bar{\rho}_i$  is the  $i$ -th Feistel operator induced by  $\rho_i$  and  $k_i$  is the  $i$ -th round key. In this setting

$$\Gamma(\Phi) = \langle \bar{\rho}_1 \sigma_{(0,k_1)} \cdots \bar{\rho}_r \sigma_{(0,k_r)} \mid (k_1, \dots, k_r) \in V^r \rangle. \quad (1)$$

**Lemma 4.1.** *If  $\Phi$  is a long-key Feistel network as above, then*

$$\langle \bar{\rho}_1 \bar{\rho}_2 \cdots \bar{\rho}_r, T(V \times V) \rangle < \Gamma(\Phi).$$

*In particular  $T(V \times V) < \Gamma(\Phi)$ .*

*Proof.* In order to prove that  $\bar{\rho}_1 \bar{\rho}_2 \cdots \bar{\rho}_r \in \Gamma(\Phi)$ , it is sufficient to consider the key  $(k_1, \dots, k_r) = (0, \dots, 0)$ . Moreover, considering the key  $(0, \dots, 0, k_r)$ , we obtain  $\bar{\rho}_1 \bar{\rho}_2 \cdots \bar{\rho}_r \sigma_{(0,k_r)} \in \Gamma(\Phi)$ , and so  $\sigma_{(0,k_r)} \in \Gamma(\Phi)$  for all  $k_r \in V$ . Finally,

$$(x_1, x_2) \begin{pmatrix} 0_n & 1_n \\ 1_n & \rho_i \end{pmatrix} \sigma_{(0,k)} = (x_2, x_1 + x_2 \rho + k) = (x_1, x_2) \sigma_{(k,0)} \begin{pmatrix} 0_n & 1_n \\ 1_n & \rho_i \end{pmatrix},$$

for any  $1 \leq i \leq r$ ,  $k \in V$  and  $(x_1, x_2) \in V \times V$ , so we have  $\bar{\rho}_i \sigma_{(0,k)} = \sigma_{(k,0)} \bar{\rho}_i$ , for any  $1 \leq i \leq r$  and  $k \in V$ . Therefore

$$\bar{\rho}_1 \sigma_{(0,k)} \bar{\rho}_2 \cdots \bar{\rho}_r = \sigma_{(k,0)} \bar{\rho}_1 \bar{\rho}_2 \cdots \bar{\rho}_r,$$

for any  $k \in V$ , and so  $\sigma_{(h,k)} \in \Gamma(\Phi)$  for any  $(h,k) \in V \times V$ . The claim then derives by the fact that  $\sigma_{(h,0)} \sigma_{(0,k)} = \sigma_{(h,k)}$ .  $\square$

In the following theorem we study which partitions can propagate in a long-key Feistel network.

**Theorem 4.2.** *Let  $\Phi$  be an  $r$ -round long-key Feistel network on  $\mathbb{M} = V \times V$ . Suppose that there exist non-trivial partitions  $\mathcal{A}$  and  $\mathcal{B}$  such that for each key  $K$  the encryption function  $E_K$  maps  $\mathcal{A}$  to  $\mathcal{B}$ . Define  $\mathcal{A}_1 = \mathcal{A}$  and  $\mathcal{A}_{i+1} = \mathcal{A}_i \bar{\rho}_i$ , for  $1 \leq i \leq r-1$ , where  $\bar{\rho}_i$  is the Feistel operator induced by the generating function  $\rho_i$  for the  $i$ -th round. Then,*

- $\mathcal{A}_{r+1} = \mathcal{B}$
- $\mathcal{A}_i$  is a linear partition, for any  $2 \leq i \leq r$ .

*Moreover, if  $\mathcal{A} = \mathcal{B}$ , i.e.  $\Gamma(\Phi)$  acts imprimitively, then  $\mathcal{A}$  is a linear partition.*

*Proof.* For any  $1 \leq i \leq r-1$  and any  $(x, y) \in V \times V$ , we have

$$\begin{aligned} (x, y) \bar{\rho}_i \sigma_{(h_i, k_i)} \bar{\rho}_{i+1} \sigma_{(0, k_{i+1})} &= (x + y \rho_i + k_i, y + h_i + (x + y \rho_i + k_i) \rho_{i+1} + k_{i+1}) \\ &= (x, y) \bar{\rho}_i \sigma_{(0, k_i)} \bar{\rho}_{i+1} \sigma_{(0, h_i + k_{i+1})}, \end{aligned}$$

and so

$$\bar{\rho}_i \sigma_{(h_i, k_i)} \bar{\rho}_{i+1} \sigma_{(0, k_{i+1})} = \bar{\rho}_i \sigma_{(0, k_i)} \bar{\rho}_{i+1} \sigma_{(0, h_i + k_{i+1})}$$

for any possible choice of  $h_i, k_i, k_{i+1} \in V$ . This implies that for any possible choice of  $h_1, k_1, \dots, h_{r-1}, k_{r-1}, k_r \in V$  the map

$$E = \bar{\rho}_1 \sigma_{(h_1, k_1)} \bar{\rho}_2 \cdots \bar{\rho}_{r-1} \sigma_{(h_{r-1}, k_{r-1})} \bar{\rho}_r \sigma_{(0, k_r)}$$

is an element of  $\Gamma(\Phi)$  as defined in Eq.(1). Therefore, for any  $1 \leq i \leq r-1$ , each possible map  $\sigma_{(h_i, k_i)} \in T(V \times V)$  appears between  $\bar{\rho}_i$  and  $\bar{\rho}_{i+1}$ , and so we



have a similar scenario of Theorem 3.3 ([5, Theorem 3.4]). Hence, proceeding as in Theorem 3.3, the desired claim follows. Moreover, if  $\mathcal{A} = \mathcal{B}$  the group  $\Gamma(\Phi)$  acts imprimitively on  $V \times V$ , since all its the generators map the partition  $\mathcal{A}$  into itself. From Lemma 4.1,  $\mathcal{A}$  is a block system also for  $T(V \times V)$ , and so, by Proposition 1,  $\mathcal{A}$  is linear.  $\square$

**Remark 1.** Note that we have defined the action of a round function of  $\Phi$  on  $V \times V$  in a such way that the corresponding round key acts on the right side of the message after applying the generating function  $\rho$  on the right factor of  $V \times V$ . In some real-case scenarios, however, it may be possible that  $\rho$  acts after the action of the corresponding round key. If this is the case, the  $i$ -th round function is defined in the following way:

$$\varepsilon_{i,K} = \sigma_{(0,k_i)} \bar{\rho}_i \sigma_{(k_i,0)}.$$

Indeed

$$\begin{aligned} (x_1, x_2) \varepsilon_{i,K} &= (x_1, x_2) \sigma_{(0,k_i)} \bar{\rho}_i \sigma_{(k_i,0)} \\ &= (x_1, x_2 + k_i) \bar{\rho}_i \sigma_{(k_i,0)} \\ &= (x_2 + k_i, x_1 + (x_2 + k_i) \rho_i) \sigma_{(k_i,0)} \\ &= (x_2, x_1 + (x_2 + k_i) \rho_i). \end{aligned}$$

In this setting we have that the group of the cipher with a long-key key-schedule is

$$G \stackrel{\text{def}}{=} \langle \sigma_{(0,k_1)} \bar{\rho}_1 \sigma_{(k_1,k_2)} \cdots \sigma_{(k_{r-1},k_r)} \bar{\rho}_r \sigma_{(k_r,0)} \mid (k_1, \dots, k_r) \in V^r \rangle,$$

and so we have  $\bar{\rho}_1 \bar{\rho}_2 \cdots \bar{\rho}_r \in G$ . We cannot prove that  $G$  contains  $T(V \times V)$  as well. Note that, as observed in the proof of Theorem 4.2, any function of the type

$$\sigma_{(0,k_1)} \bar{\rho}_1 \sigma_{(k_1,k_2)} \cdots \sigma_{(k_{r-1},k_r)} \bar{\rho}_r \sigma_{(k_r,0)}$$

can be represented as a function of type

$$\sigma_{(0,k_1)} \bar{\rho}_1 \sigma_{(0,k_2)} \bar{\rho}_2 \sigma_{(0,k_1+k_2)} \cdots \sigma_{(0,k_{r-2}+k_r)} \bar{\rho}_r \sigma_{(k_r,k_{r-1})},$$

which is an element of  $\Gamma(\Phi)$ , recalling that  $\Phi$  represents the cipher where the key addition is applied after the generating function. Thus, studying the properties of  $\Gamma(\Phi)$  gives also important informations on  $G$ , e.g. if  $\Gamma(\Phi)$  acts imprimitively, then so does  $G$ . More in general, partitions for  $\Gamma(\Phi)$  are also partition for  $G$ .

In what follows, we aim at studying algebraic conditions which need to be satisfied by some partitions to prevent the partition-based attack. In particular, we classify a family of block systems which, in the case of Feistel networks, cannot be exploited for partition-based cryptanalysis. It is important to point out that the considered set of block systems contains the most used type of partitions for cryptanalysis. In order to do so, we need to study the subgroups of the direct product  $(V \times V, +)$ . We make use of the following result, due to Goursat [16, Sections 11–12], which characterises the subgroups of the direct product of two groups in terms of suitable sections of the direct factors (see also [20]).

**Theorem 4.3** (Goursat's Lemma [16]). *Let  $G_1$  and  $G_2$  be two groups. There exists a bijection between*

1. *the set of all subgroups of the direct product  $G_1 \times G_2$ , and*
2. *the set of all triples  $(A/B, C/D, \psi)$ , where*
  - *$A$  is a subgroup of  $G_1$ ,*
  - *$C$  is a subgroup of  $G_2$ ,*

- $B$  is a normal subgroup of  $A$ ,
- $D$  is a normal subgroup of  $C$ , and
- $\psi : A/B \rightarrow C/D$  is a group isomorphism.

In this bijection, each subgroup of  $G_1 \times G_2$  can be uniquely written as

$$U_\psi = \{(a, c) \in A \times C : (a + B)\psi = c + D\}.$$

Note that the isomorphism  $\psi : A/B \rightarrow C/D$  is induced by a homomorphism  $\varphi : A \rightarrow C$  such that  $(a + B)\psi = a\varphi + D$  for any  $a \in A$ , and  $B\varphi \leq D$ . Such homomorphism is not unique.

**Lemma 4.4** ([3]). *In the above notation, given any homomorphism  $\varphi$  inducing  $\psi$ , we have*

$$U_\psi = \{(a, a\varphi + d) : a \in A, d \in D\}. \quad (2)$$

*Proof.* Note first that the right-hand side of (2) is contained in  $U_\psi$ , since for  $a \in A$  and  $d \in D$  we have  $(a + B)\psi = a\varphi + D = a\varphi + d + D$ , that is,  $(a, a\varphi + d) \in U_\psi$ . Moreover  $U_\psi$  is contained in the right-hand side of (2). Indeed, if  $(a, c) \in U_\psi$  we have  $a\varphi + D = (a + B)\psi = c + D$ , so that  $c = a\varphi + d$  for some  $d \in D$ .  $\square$

In the following result we consider two subgroups of  $V \times V$  such that the first is mapped into the second by a Feistel operator. We highlight some condition that such subgroups have to satisfy. We will use the conditions derived from the next lemma also in Theorem 4.6 and in Theorem 4.8.

**Lemma 4.5.** *Let  $\rho \in \text{Sym}(V)$  be such that  $0\rho = 0$  and let  $\bar{\rho}$  be the corresponding Feistel operator. Suppose that there exist two subgroups  $\mathcal{U}_1 = \{(a_1, a_1\varphi_1 + d_1) \mid a_1 \in A_1, d_1 \in D_1\}$  and  $\mathcal{U}_2 = \{(a_2, a_2\varphi_2 + d_2) \mid a_2 \in A_2, d_2 \in D_2\}$ ,  $\mathcal{U}_1, \mathcal{U}_2 \leq V \times V$ , where  $A_i, D_i$  and  $\varphi_i$  are as in Lemma 4.4, such that*

$$\mathcal{U}_1\bar{\rho} = \mathcal{U}_2.$$

The following properties hold true:

1.  $\text{Ker } \varphi_1 \leq D_2$ ;
2.  $D_2 \leq A_1$ ;
3.  $A_2 = A_1\varphi_1 + D_1$ ;
4.  $D_2\varphi_1 \leq D_1$ .

Moreover,

- (i) if  $D_1 = \{0\}$  and  $D_2 = \{0\}$ , then  $\rho$  is linear on  $A_2$ ;
- (ii) if  $\mathcal{U}_1 = A_1 \times D_1$  and  $\mathcal{U}_2 = A_2 \times D_2$ , then  $D_1 = A_2$  and  $D_2 = A_1$ .

*Proof.* By assumption, for any  $a_1 \in A_1$  and  $d_1 \in D_1$  there exist  $x_2 \in A_2$  and  $y_2 \in D_2$  such that

$$(a_1, a_1\varphi_1 + d_1) \begin{pmatrix} 0_n & 1_n \\ 1_n & \rho \end{pmatrix} = (x_2, x_2\varphi_2 + y_2),$$

that is

$$(a_1\varphi_1 + d_1, a_1 + (a_1\varphi_1 + d_1)\rho) = (x_2, x_2\varphi_2 + y_2).$$

From this we derive  $a_1\varphi_1 + d_1 = x_2$  and so  $A_1\varphi_1 + D_1 \leq A_2$ . Moreover, since  $\varphi_1$  is a homomorphism, we have

$$a_1 + (a_1\varphi_1 + d_1)\rho = a_1\varphi_1\varphi_2 + d_1\varphi_2 + y_2,$$

hence, considering  $d_1 = 0$  and  $a_1 \in \text{Ker } \varphi_1$ , we obtain  $\text{Ker } \varphi_1 \leq D_2$ . Similarly, from  $\mathcal{U}_2 \bar{\rho}^{-1} = \mathcal{U}_1$ , we obtain that for any  $a_2 \in A_2$  and  $d_2 \in D_2$  there exist  $x_1 \in A_1$  and  $y_1 \in D_1$  such that

$$(a_2, a_2\varphi_2 + d_2) \begin{pmatrix} \rho & 1_n \\ 1_n & 0_n \end{pmatrix} = (x_1, x_1\varphi_1 + y_1),$$

that is

$$(a_2\rho + a_2\varphi_2 + d_2, a_2) = (x_1, x_1\varphi_1 + y_1). \quad (3)$$

From this it follows  $a_2\rho + a_2\varphi_2 + d_2 \in A_1$ , and considering  $a_2 = 0$  we have  $d_2 \in A_1$  for any  $d_2 \in D_2$ , and so  $D_2 \leq A_1$ . Moreover, since  $a_2 = x_1\varphi_1 + y_1$ , we have  $A_2 \leq A_1\varphi_1 + D_1$ , and so  $A_1\varphi_1 + D_1 = A_2$ . By Eq.(3), we also obtain

$$a_2 + (a_2\rho + a_2\varphi_2 + d_2)\varphi_1 = d_1,$$

from which it follows that  $D_2\varphi_1 \leq D_1$ , considering  $a_2 = 0$ .

If  $D_1 = D_2 = \{0\}$ , since  $\text{Ker } \varphi_1 \leq D_2$ , we have that  $\varphi_1$  is an isomorphism. Then from (3) we obtain

$$a_2\rho = a_2\varphi_2 + a_2\varphi_1^{-1},$$

for any  $a_2 \in A_2$ . The last equation implies that  $\rho$  acts linearly over  $A_2$ .

If  $\mathcal{U}_1 = A_1 \times D_1$  and  $\mathcal{U}_2 = A_2 \times D_2$ , then  $A_1\varphi_1 \leq D_1$  and  $A_2\varphi_2 \leq D_2$ . So  $A_2 = D_1$ , since  $A_2 = A_1\varphi_1 + D_1$ . Finally, since  $(a_1, 0)\bar{\rho} = (0, a_1)$  we obtain that  $A_1 \leq D_2$ , and so  $A_1 = D_2$ .  $\square$

In the following theorem we show that the study of the partition propagation after two rounds of a Feistel network can be reduced to the study of the partition propagation in a round of the corresponding SPN. A similar argument is used to provide a reduction from the primitivity of the group generated by a Feistel network to the one of the related SPN [1].

**Theorem 4.6.** *Let  $\rho_1, \rho_2 \in \text{Sym}(V) \setminus \text{AGL}(V)$  and let  $\bar{\rho}_1$  and  $\bar{\rho}_2$  be the corresponding Feistel operators. Suppose that there exist two non-trivial and proper subgroups  $\mathcal{U}_1$  and  $\mathcal{U}_2$  of  $V \times V$  such that*

1. *for each  $(v_1, w_1) \in V \times V$  there exists  $(v_2, w_2) \in V \times V$  such that*

$$(\mathcal{U}_1 + (v_1, w_1))\bar{\rho}_1 = \mathcal{U}_2 + (v_2, w_2),$$

2. *for each  $(v_2, w_2) \in V \times V$  there exists  $(v_1, w_1) \in V \times V$  such that*

$$(\mathcal{U}_2 + (v_2, w_2))\bar{\rho}_2 = \mathcal{U}_1 + (v_1, w_1).$$

*Then there exist  $U_1$  and  $W_1$  non-trivial and proper subgroups of  $V$  such that for each  $v \in V$  there exists  $w \in V$  such that*

$$(U_1 + v)\rho_1 = W_1 + w.$$

*Analogously, then there exist  $U_2$  and  $W_2$  non-trivial and proper subgroups of  $V$  such that for each  $v \in V$  there exists  $w \in V$  such that*

$$(U_2 + v)\rho_2 = W_2 + w.$$

*Proof.* By Lemma 4.4 we have

$$\mathcal{U}_i = \{(a_i, a_i\varphi_i + d_i) \mid a_i \in A_i \text{ and } d_i \in D_i\}$$

for each  $i = 1, 2$ . What follows from now on holds for both  $i = 1$  and  $i = 2$ , where if  $i = 2$  we consider  $i + 1$  as  $(i + 1) \bmod 2 = 1$ . We can assume without loss of generality that  $0\rho_1 = 0\rho_2 = 0$ . Using assumptions 1. and 2., applying Lemma 4.5 we obtain  $A_{i+1} = A_i\varphi_i + D_i$ ,  $D_{i+1}\varphi_i \leq D_i$  and  $\text{Ker } \varphi_i \leq D_{i+1}$ . Since

$(v, w) \begin{pmatrix} 0_n & 1_n \\ 1_n & \rho_i \end{pmatrix} = (w, v + w\rho_i)$  for each  $(v, w) \in V \times V$ , in assumptions 1. and 2. we can assume  $v_{i+1} = w_i$  and  $w_{i+1} = v_i + w_i\rho_i$ . Therefore, in the general case, for any  $a_i \in A_i$ ,  $d_i \in D_i$  and  $(v_i, w_i) \in V \times V$  there exist  $x_{i+1} \in A_{i+1}$  and  $y_{i+1} \in D_{i+1}$  such that

$$(a_i + v_i, a_i\varphi_i + d_i + w_i) \begin{pmatrix} 0_n & 1_n \\ 1_n & \rho_i \end{pmatrix} = (x_{i+1} + w_i, x_{i+1}\varphi_{i+1} + y_{i+1} + v_i + w_i\rho_i)$$

that is, since the maps  $\varphi_i$  are homomorphisms,

$$a_i + (a_i\varphi_i + d_i + w_i)\rho_i = a_i\varphi_i\varphi_{i+1} + d_i\varphi_{i+1} + y_{i+1} + w_i\rho_i.$$

Hence, considering  $a_i = 0$ , it follows that

$$(D_i + w_i)\rho_i \leq D_{i+1} + w_i\rho_i,$$

yielding  $|D_i| \leq |D_{i+1}|$  for  $i \in \{1, 2\}$ , therefore  $|D_1| = |D_2|$ . Consequently, for  $i \in \{1, 2\}$  we obtain

$$(D_i + w_i)\rho_i = D_{i+1} + w_i\rho_i. \quad (4)$$

From this the desired result follows, provided that  $D_i$  and  $D_{i+1}$  are both different from  $(\mathbb{F}_2)^n$  and both different from  $\{0\}$ . First note that  $D_i = (\mathbb{F}_2)^n$  if and only if  $D_{i+i} = (\mathbb{F}_2)^n$ . Analogously  $D_i = \{0\}$  if and only if  $D_{i+i} = \{0\}$ .

**[ $\mathbf{D}_i = (\mathbb{F}_2)^n$ ]** Since  $D_1 \leq A_2$  and  $D_2 \leq A_1$ , we have  $A_2 = (\mathbb{F}_2)^n = A_1$ . Therefore  $C_i = B_i = (\mathbb{F}_2)^n$  for  $i = \{1, 2\}$ , since  $A_i/B_i \cong C_i/D_i$ , and so  $\mathcal{U}_i$  is trivial, a contradiction.

**[ $\mathbf{D}_i = \{0\}$ ]** Since  $\text{Ker } \varphi_1 \leq D_2 = \{0\}$  and  $\text{Ker } \varphi_2 \leq D_1 = \{0\}$ , we have that

$$\psi_i = \varphi_i : A_i \xrightarrow{\cong} C_i$$

is an isomorphism. Therefore

$$A_i \cong C_i = A_i\varphi_i = A_{i+1} \cong C_{i+1} = A_{i+1}\varphi_{i+1}$$

and in particular  $|A_i| = |A_{i+1}|$ .

Since  $D_i = D_{i+1} = \{0\}$ , for any  $a_i \in A_i$  and  $(v_i, w_i) \in V \times V$  there exists  $x_{i+1} \in A_{i+1}$  such that

$$(a_i + v_i, a_i\varphi_i + w_i) \begin{pmatrix} 0_n & 1_n \\ 1_n & \rho_i \end{pmatrix} = (x_{i+1} + w_i, x_{i+1}\varphi_{i+1} + v_i + w_i\rho_i),$$

that is

$$a_i + (a_i\varphi_i + w_i)\rho_i = a_i\varphi_i\varphi_{i+1} + w_i\rho_i. \quad (5)$$

If  $A_i = \{0\}$ , then  $C_i = \{0\}$  and so  $\mathcal{U}_i$  is trivial, a contradiction. Otherwise, if  $A_i = (\mathbb{F}_2)^n$ , then  $A_i\varphi_i = A_{i+1} = (\mathbb{F}_2)^n$  and  $a_i\varphi_i + w_i$  is an element of  $A_{i+1} = (\mathbb{F}_2)^n$ . Hence in Eq. (5) we can consider  $w_i = 0$ , obtaining

$$a_i + (a_i\varphi_i)\rho_i = a_i\varphi_i\varphi_{i+1}.$$

Since the function  $x \mapsto x + x\varphi_i\varphi_{i+1}$  is linear, we proved that  $\rho_i \in \text{AGL}(V)$ , which is a contradiction since by hypothesis we are assuming  $\rho_i \in \text{Sym}(V) \setminus \text{AGL}(V)$ .

If  $A_i < (\mathbb{F}_2)^n$ , for  $i \in \{1, 2\}$  we obtain

$$(a_i\varphi_i + w_i)\rho_i = a_i + a_i\varphi_i\varphi_{i+1} + w_i\rho_i.$$

Since  $a_i$  and  $a_i\varphi_i\varphi_{i+1}$  is contained in  $A_i$  and  $a_i\varphi_i$  is an element of  $A_{i+1}$  for each  $a_i \in A_i$ , and  $|A_i| = |A_{i+1}|$ , then by Eq. (5) we obtain

$$(A_{i+1} + w_i)\rho_i = A_i + w_i\rho_i, \quad (6)$$

with  $A_i, A_{i+1} < (\mathbb{F}_2)^n$ . This concludes the proof: indeed, if  $D_1$  and  $D_2$  are both proper and non-trivial subgroups of  $V$ , the claim follows from Eq. (4). Otherwise, the claim follows from Eq. (6).  $\square$

The following result examines the converse implication of Theorem 4.6.

**Theorem 4.7.** *Let  $\rho \in \text{Sym}(V)$  and let  $\bar{\rho}$  be the corresponding Feistel operator. If there exist  $\mathcal{L}(U_1)$  and  $\mathcal{L}(U_2)$  non-trivial linear partitions of  $V$  such that  $\mathcal{L}(U_1)\rho = \mathcal{L}(U_2)$ , then there exist two non-trivial linear partitions of  $V \times V$  such that  $\mathcal{L}(\mathcal{U}_1)\bar{\rho} = \mathcal{L}(\mathcal{U}_2)$ .*

*Proof.* Since  $\mathcal{L}(U_1)\rho = \mathcal{L}(U_2)$ , for each  $v \in V$  there exists  $w \in V$  such that

$$(U_1 + v)\rho = U_2 + w. \quad (7)$$

Notice that in Eq. (7) we can choose  $w = v\rho$ .

Let  $\mathcal{U}_1 \stackrel{\text{def}}{=} \{(u, u') \in U_2 \times U_1\}$  and  $\mathcal{U}_2 \stackrel{\text{def}}{=} \{(u, u') \in U_1 \times U_2\}$ . Since  $U_1, U_2$  are not trivial, then also  $\mathcal{U}_1$  and  $\mathcal{U}_2$  are non-trivial. Let  $(u, u') \in \mathcal{U}_1$  and  $(v, v') \in V \times V$ , then we have

$$(u + v, u' + v')\bar{\rho} = (u + v, u' + v') \begin{pmatrix} 0_n & 1_n \\ 1_n & \rho \end{pmatrix} = (u' + v', u + v + (u' + v')\rho).$$

By Eq. (7), there exists  $u'' \in U_2$  such that  $(u' + v')\rho = u'' + v'\rho$  and so for each  $(u, u') \in \mathcal{U}_1$  and  $(v, v') \in V \times V$  we obtain

$$(u + v, u' + v')\bar{\rho} = (u' + v', (u + u'') + v + v'\rho) \in (U_1 + v') \times (U_2 + v + v'\rho).$$

Since  $(U_1 + v') \times (U_2 + v + v'\rho) = \mathcal{U}_2 + (v', v + v'\rho)$ , we have

$$(\mathcal{U}_1 + (v, v'))\bar{\rho} \subseteq \mathcal{U}_2 + (v', v + v'\rho)$$

and so

$$(\mathcal{U}_1 + (v, v'))\bar{\rho} = \mathcal{U}_2 + (v', v + v'\rho)$$

since  $|\mathcal{U}_1| = |(\mathcal{U}_1 + (v, v'))\bar{\rho}| = |\mathcal{U}_2 + (v', v + v'\rho)| = |\mathcal{U}_2|$ .  $\square$

**Remark 2.** Notice that if  $U_1 = U_2$  then  $\mathcal{U}_1 = \mathcal{U}_2$ . In this case, Theorem 4.7 provides the converse of Theorem 4.5 proved in [1]. In other words, the primitivity of the group  $\langle \rho, T(V) \rangle$  is a necessary and sufficient condition for the primitivity of the group generated by the round functions of the Feistel network acting on  $V \times V$  and having  $\rho$  as generating function for each round.

As announced, we provide a partial generalisation of Theorem 3.4 in the Feistel network case. In particular, we show some types of block systems which are not usable for the purpose of the partition-based cryptanalysis. More precisely, we show that if a Feistel network has a sequence of non-trivial linear partitions which propagate from the first round to the last one, then such partitions cannot be of the type specified in the following theorem. In other words, we are studying the propagation of linear partitions under the action of  $r$  rounds, where each possible key can be chosen, i.e. under the action of a long-key Feistel network. The considered Feistel network has a generating function which is the composition of a parallel S-box followed by a diffusion layer, i.e. an SPN-like generating function. The same notation of Lemma 4.4 is used in the following result.

**Theorem 4.8.** *Let  $\rho_1, \dots, \rho_r \in \text{Sym}(V)$  and let  $\Phi$  be the  $r$ -round Feistel network where the  $i$ -th round applies the Feistel operator  $\bar{\rho}_i$  induced by  $\rho_i$ . Let us assume that  $0\rho_i = 0$  and  $\rho_i = \gamma_i\lambda_i$ , where*

- a)  $\gamma_i$  is a parallel map which applies  $2^\delta$ -differentially uniform and  $(\delta-1)$ -strongly anti-invariant S-boxes, for some  $\delta < s$ , where  $s$  denotes the dimension of each brick,
- b)  $\lambda_i$  a linear strongly-proper diffusion layer.

Suppose that there exists a sequence of  $r+1$  non-trivial linear partitions  $\mathcal{L}(\mathcal{U}_1), \dots, \mathcal{L}(\mathcal{U}_{r+1})$ , where  $\mathcal{U}_i$  is a proper and non-trivial subgroup of  $V \times V$  and  $\mathcal{L}(\mathcal{U}_i)\bar{\rho}_i = \mathcal{L}(\mathcal{U}_{i+1})$  for all  $1 \leq i \leq r$ . Then, none of the following condition is satisfied:

1. there exists  $1 \leq i \leq r-1$  such that  $\mathcal{L}(\mathcal{U}_{i+1})\bar{\rho}_{i+1} = \mathcal{L}(\mathcal{U}_i)$ ,
2. there exists  $1 \leq i \leq r-1$  such that  $\mathcal{U}_i = A_i \times D_i$ ,  $\mathcal{U}_{i+1} = A_{i+1} \times D_{i+1}$  and  $\mathcal{U}_{i+2} = A_{i+2} \times D_{i+2}$ ,
3. there exists  $1 \leq i \leq r$  such that  $D_i = \{0\}$  and  $D_{i+1} = \{0\}$ ,
4. there exists  $1 \leq i \leq r$  such that  $A_i = \{0\}$  and  $A_{i+1} = \{0\}$ .

*Proof.* We proceed in each case by contradiction.

1. Let  $1 \leq i \leq r-1$  such that  $\mathcal{L}(\mathcal{U}_{i+1})\bar{\rho}_{i+1} = \mathcal{L}(\mathcal{U}_i)$ . Then, by Theorem 4.6, there exist  $U_i$  and  $U_{i+1}$  subgroups of  $V$  such that  $\mathcal{L}(U_i)\rho_i = \mathcal{L}(U_{i+1})$  and  $\mathcal{L}(U_{i+1})\rho_{i+1} = \mathcal{L}(U_i)$ . Then, by Proposition 2,  $U_i$  and  $U_{i+1}$  are walls and  $U_{i+1} = U_i\lambda_i$ , which contradicts the fact that  $\lambda_i$  is strongly proper.
2. Let  $1 \leq i \leq r-1$  such that  $\mathcal{U}_i = A_i \times D_i$ ,  $\mathcal{U}_{i+1} = A_{i+1} \times D_{i+1}$  and  $\mathcal{U}_{i+2} = A_{i+2} \times D_{i+2}$ . By Lemma 4.5,  $\mathcal{U}_i = A_i \times A_{i+1}$ ,  $\mathcal{U}_{i+1} = A_{i+1} \times A_i$  and  $\mathcal{U}_{i+2} = A_i \times A_{i+1}$ . This contradicts what previously proved.
3. Let  $1 \leq i \leq r$  such that  $D_i = D_{i+1} = \{0\}$ , which implies  $\mathcal{U}_i = \{(a_i, a_i\varphi_i) : a_i \in A_i\}$  and  $\mathcal{U}_{i+1} = \{(a_{i+1}, a_{i+1}\varphi_{i+1}) : a_{i+1} \in A_{i+1}\}$ . If  $A_i = \{0\}$ , then  $\mathcal{U}_i$  is trivial. Since  $D_i = D_{i+1} = \{0\}$  and  $\text{Ker } \varphi_i \leq D_{i+1}$ , we have that  $\varphi_i$  is an isomorphism over  $A_i$  and  $A_i\varphi_i = A_{i+1}$ . Moreover, by Lemma 4.5,  $\rho_i$  is linear over  $A_{i+1}$ . If  $A_i = (\mathbb{F}_2)^n$ , then  $\gamma_i$  is linear on  $V$ , which contradicts the fact that  $\gamma_i$  satisfies the conditions in a). Suppose now  $A_i < (\mathbb{F}_2)^n$ . As in the proof of Theorem 4.6 we obtain that

$$(A_{i+1} + w_i)\rho_i = A_i + w_i\rho_i$$

for any  $w_i$  in  $(\mathbb{F}_2)^n$ . Then  $\gamma_i$  maps the linear partition  $\mathcal{L}(A_{i+1})$  into  $\mathcal{L}(A_i\lambda_i^{-1})$ . By Proposition 2,  $A_{i+1} = A_i\lambda_i^{-1}$ , and  $A_{i+1}$  is a wall. Since  $\rho_i$  is linear over  $A_{i+1}$ , then  $\gamma_i$  is linear over  $A_{i+1}$ . If  $V_j$  be a brick of the wall  $A_{i+1}$ , then the S-box of  $\gamma_i$  relative to the brick  $V_j$  is a linear map over  $V_j$ , which is a contradiction.

4. Let  $1 \leq i \leq r$  such that  $A_i = A_{i+1} = \{0\}$ . By Lemma 4.5,  $D_{i+1} \leq A_i = \{0\}$ , hence  $\mathcal{U}_i$  is trivial.  $\square$

It is worth noticing that the partition used by Paterson in his construction of a DES-like trapdoor cipher (see [19, Lemma 3]) is as in point 2 in the previous theorem.

We conclude this section by observing that it is possible to prove a result similar to Theorem 4.8 using a weaker notion of differential uniformity, defined in [11], provided a larger value of strong anti-invariance. Recalling that a map  $f \in \text{Sym}((\mathbb{F}_2)^s)$  is said to be *weakly  $\delta$ -uniform* if for each  $a \in (\mathbb{F}_2)^s \setminus \{0\}$  we have

$$|\{xf + (x+a)f \mid x \in (\mathbb{F}_2)^s\}| > \frac{2^{s-1}}{\delta},$$

the following alternative result is easily checked. Its proof is obtained reasoning as in the proof of Theorem 4.8, since Proposition 2 is still valid if one assumes that the S-boxes are weakly  $2^\delta$ -uniform and  $\delta$ -strongly anti-invariant.

**Theorem 4.9.** *Let  $\rho_1, \dots, \rho_r \in \text{Sym}(V)$  and let  $\Phi$  be the  $r$ -round Feistel network where the  $i$ -th round applies the Feistel operator  $\bar{\rho}_i$  induced by  $\rho_i$ . Let us assume that  $0\rho_i = 0$  and  $\rho_i = \gamma_i\lambda_i$ , where*

- a)  $\gamma_i$  is a parallel map which applies weakly  $2^\delta$ -uniform and  $\delta$ -strongly anti-invariant S-boxes, for some  $\delta < s$ ,
- b)  $\lambda_i$  a linear strongly-proper diffusion layer.

*Suppose that there exists a sequence of  $r + 1$  non-trivial linear partitions  $\mathcal{L}(\mathcal{U}_1), \dots, \mathcal{L}(\mathcal{U}_{r+1})$ , where  $\mathcal{U}_i$  is a proper and non-trivial subgroup of  $V \times V$  and  $\mathcal{L}(\mathcal{U}_i)\bar{\rho}_i = \mathcal{L}(\mathcal{U}_{i+1})$  for all  $1 \leq i \leq r$ . Then, none of the following condition is satisfied:*

- 1. *there exists  $1 \leq i \leq r - 1$  such that  $\mathcal{L}(\mathcal{U}_{i+1})\bar{\rho}_{i+1} = \mathcal{L}(\mathcal{U}_i)$ ,*
- 2. *there exists  $1 \leq i \leq r - 1$  such that  $\mathcal{U}_i = A_i \times D_i$ ,  $\mathcal{U}_{i+1} = A_{i+1} \times D_{i+1}$  and  $\mathcal{U}_{i+2} = A_{i+2} \times D_{i+2}$ ,*
- 3. *there exists  $1 \leq i \leq r$  such that  $D_i = \{0\}$  and  $D_{i+1} = \{0\}$ ,*
- 4. *there exists  $1 \leq i \leq r$  such that  $A_i = \{0\}$  and  $A_{i+1} = \{0\}$ .*

**5. Conclusions and open problems.** In this work, partition propagation under the action of a long-key Feistel network has been investigated, and some previous results [5, 6, 9] set in a long-key SPN scenario have been generalized. In details, we proved that only linear partitions can propagate under the action of a long-key Feistel network. Moreover, we presented some types of block systems which are not usable for the purpose of the partition-based cryptanalysis. In other words, we showed that if in a long-key Feistel network a sequence of non-trivial linear partitions propagate from the first round to the last one, then such partitions cannot be of some types used in specific attacks (see e.g. [19]).

The problem of giving a complete generalisation of Theorem 3.4 of [9] to the case of Feistel networks is still open. Moreover, the optimal result that a block-cipher designer can achieve in terms of group-theoretical security is to obtain a cipher whose corresponding group is the larger possible. For this reason, we aim at studying which conditions imply that the group of the encryption functions of a long-key cipher is the alternating or symmetric group, both in case of SPNs and Feistel networks.

**Acknowledgement.** We would like to express our gratitude to the anonymous referees for their valuable comments and suggestions.

**References**

- [1] R. Aragona, M. Calderini, R. Civino, M. Sala, I. Zappatore, Wave-Shaped Round Functions and Primitive Groups, *Advances in Mathematics of Communications*, **13** (2019), 67–88.
- [2] R. Aragona, M. Calderini, A. Tortora and M. Tota, On the primitivity of PRESENT and other lightweight ciphers, *J. Algebra Appl.*, **17** (2017), 1850115 (16 pages).
- [3] R. Aragona, A. Caranti and M. Sala, The group generated by the round functions of a GOST-like cipher, *Ann. Mat. Pura Appl.*, **196** (2016), 1–17.
- [4] R. Aragona, A. Caranti, F. Dalla Volta and M. Sala, On the group generated by the round functions of translation based ciphers over arbitrary fields, *Finite Fields Appl.*, **25** (2014), 293–305.

- [5] A. Banner, N. Bodin and E. Filiol, Partition-Based Trapdoor Ciphers, *Cryptology ePrint Archive*, Report 2016/493, 2016.
- [6] A. Banner, and E. Filiol, *Partition-based trapdoor ciphers*, IntechOpen, London, 2017.
- [7] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems, *Journal of CRYPTOLOGY*, **4** (1991), 3–72.
- [8] A. Bogdanov et al., PRESENT: An ultra-lightweight block cipher, *CHES '07*, Lecture Notes in Comput. Sci., **4727** (2007), 450–466.
- [9] M. Calderini, A note on some algebraic trapdoors for block ciphers, *Advances in Mathematics of Communications*, **12** (2018), 515–524.
- [10] M. Calderini, R. Civino and M. Sala, On properties of translation groups in the affine general linear group with applications to cryptography, preprint, [arXiv:math.GR/1702.00581](https://arxiv.org/abs/math/1702.00581), 2017.
- [11] A. Caranti, F. Dalla Volta and M. Sala, On some block ciphers and imprimitive groups, *Appl. Algebra Engrg. Comm. Comput.*, **20** (2009), 339–350.
- [12] 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, *Des. Codes Cryptogr.*, **52** (2009), 293–301.
- [13] D. Coppersmith and E. Grossman, Generators for certain alternating groups with applications to cryptography, *SIAM J. Appl. Math.*, **29** (1975), 624–627.
- [14] J. Daemen and V. Rijmen, *The design of Rijndael: AES – the Advanced Encryption Standard*, Information Security and Cryptography, Springer-Verlag, Berlin, 2002.
- [15] Federal information processing standards publication, *Data Encryption Standard and others*, National Bureau of Standards, US Department of Commerce, 1977.
- [16] E. Goursat, Sur les substitutions orthogonales et les divisions régulières de l’espace, *Ann. Sci. École Norm. Sup.*, **3** (1889), 9–102.
- [17] C. Harpes and J. L. Massey, Partitioning cryptanalysis, *Fast Software Encryption*, Lecture Notes in Comput. Sci., **1267** (1997), 13–27.
- [18] Jr. B. S. Kaliski, R. L. Rivest and A. T. Sherman, Is the Data Encryption Standard a group? (Results of cycling experiments on DES), *J. Cryptology*, **1** (1988), 3–36.
- [19] K. G. Paterson, Imprimitive permutation groups and trapdoors in iterated block ciphers, *Fast Software Encryption*, Lecture Notes in Comput. Sci., **1636** (1999), 201–214.
- [20] J. Petrillo, Goursat’s other theorem, *The College Mathematics Journal*, **40**(2009), 119–124.
- [21] C. E. Shannon, Communication theory of secrecy systems, *Bell System Tech.*, **28** (1949), 656–715.
- [22] R. Sparr and R. Wernsdorf, Group theoretic properties of Rijndael-like ciphers, *Discrete Appl. Math.*, **156** (2008), 3139–3149.
- [23] R. Wernsdorf, The round functions of RIJNDAEL generate the alternating group, *Fast Software Encryption*, Lecture Notes in Comput. Sci., **2365** (2002), 143–148.
- [24] R. Wernsdorf, The round functions of SERPENT generate the alternating group, 2000. Available from: <http://csrc.nist.gov/archive/aes/round2/comments/20000512-rwernsdorf.pdf>.
- [25] R. Wernsdorf, The one-round functions of the DES generate the alternating group, *Advances in Cryptology-EUROCRYPT '92*, Lecture Notes in Comput. Sci., **658** (1993), 99–112.

Received xxxx 20xx; revised xxxx 20xx.

E-mail address: [riccardo.aragona@univaq.it](mailto:riccardo.aragona@univaq.it)

E-mail address: [marco.calderini@uib.no](mailto:marco.calderini@uib.no)

E-mail address: [roberto.civino@univaq.it](mailto:roberto.civino@univaq.it)