Linear Structures in Blockciphers[1]

Jan-Hendrik Evertse
University of Leiden, Department of Mathematics and Computer Science
P.O. Box 9512, 2300 RA Leiden, The Netherlands

1. Introduction

In this paper, we deal with certain cryptographic functions, called 'blockciphers', and introduce certain weaknesses that blockciphers might have, named 'linear structures.' It is explained that blockciphers can be broken more easily if they possess linear structures. In particular, we pay attention to the Data Encryption Standard, which is a blockcipher used in the USA as a standard for the encryption of data for civil use. This paper will also appear in a somewhat different form in [8].

In the first part of the introduction, we introduce some terminology to make the paper more easily readable for the non-specialist. In the meanwhile we discuss some of the history of our subject. In the second part of the introduction, we give a brief overview of the contents of the paper.

1.1. History and terminology

Mathematically speaking, a blockcipher is a mapping $F: \{0,1\}^m \times \{0,1\}^k \to \{0,1\}^m$ such that for each $\mathbf{k}$ in $\{0,1\}^k$, the mapping $F(\cdot,\mathbf{k}): \{0,1\}^m \to \{0,1\}^m$ is one-to-one. If $\mathbf{c}=F(\mathbf{p},\mathbf{k})$ then $\mathbf{p}$, $\mathbf{k}$ and $\mathbf{c}$ are called the plaintext, key and ciphertext, respectively, and the coordinates of $\mathbf{p}$, $\mathbf{k}$ and $\mathbf{c}$ are called plaintext bits, key bits and ciphertext bits. m and k are called the message length and key length, respectively of F. Blockciphers are mostly used as *secret key cryptosystems.* When two parties A and B want to communicate

1. This research was supported by the Netherlands Organization for the Advancement of Pure Research (Z.W.O.), and was carried out at the Centrum voor Wiskunde en Informatica.

over an insecure channel, they agree in advance about a key $\mathbf{k}$ that is kept secret from outsiders. Whenever A wants to send a message to B, consisting of zeros or ones, then A partitions that message into blocks of length m, encrypts each block by applying $F(.,\mathbf{k})$ to it, and sends the encrypted blocks to B. Then B decrypts the encrypted blocks by applying $F(.,\mathbf{k})^{-1}$ to them. (There are more secure ways to encrypt messages by means of blockciphers, cf. [14], which are not discussed here.)

We assume that the mapping F is public. Thus, the communication between A and B cannot be secure if an adverse cryptanalist is able to find the key A and B agreed upon. The methods by which a cryptanalist could try to find the key used by A and B are usually divided into three classes, depending on the information that the cryptanalist can obtain.

Ciphertext only attacks. The cryptanalist tries to find the key by using some ciphertexts (which he may have obtained by eavesdropping the communication between A and B over the insecure channel) and some statistical properties of the corresponding plaintexts (e.g. when the plaintext is English text).

Known plaintext attacks. If the cryptanalist intercepts some ciphertexts $\mathbf{c}$, and some of the corresponding plaintexts $\mathbf{p}$ become public after some time, then he could try to find the unknown key $\mathbf{k}$ by solving $\mathbf{k}$ from the equations $F(\mathbf{p},\mathbf{k})=\mathbf{c}$. A trivial known plaintext attack is *'exhaustive key search'*: the cryptanalist takes some plaintext $\mathbf{p}$ of which he knows the corresponding ciphertext $\mathbf{c}$ and tries all keys $\mathbf{k}$ until he finds one with $F(\mathbf{p},\mathbf{k})=\mathbf{c}$.

Chosen plaintext attacks. The cryptanalist is able to obtain the ciphertexts corresponding to special plaintexts chosen by himself, and may use these plaintexts and ciphertexts to search for the key.

Probably the best known blockcipher is the NBS Data Encryption Standard (DES), with message length 64 and key length 56. DES is the iteration of sixteen 'simple' blockciphers (rounds). These blockciphers are all the same, except that they use different 'subkeys' of length 48 which are extracted from the key of length 56 of the whole DES. Each round of DES is built up from 'bit permutations' that permute the bits of the input, 'permuted choices' that select some of the bits of the input and permute the selected bits in some order, an 'extension', that makes the input longer by duplicating some of its bits, and 'S-boxes' that map blocks of six bits onto blocks of four bits. Further, each round of DES is 'self-inverse', so that DES-decryptions can be done by performing the sixteen rounds in opposite order. For the precise description of DES we refer to [13]. The DES-algorithm was developed by IBM and published in 1975. At the advice of the US National Security Agency (NSA), the algorithm was accepted in 1977 as a US standard for the encryption of data for civil use by the US National Bureau of Standards (NBS). Although DES itself was published in full detail, its design criteria were kept secret, at the instigation of NSA. This led to a considerable

research on DES, and to blockciphers in general. Especially the S-boxes of DES were investigated thoroughly, since these are mainly responsible for the strength of DES. Interested readers will find many facts about the S-boxes in [10], [4], [5] and [1].

One of the peculiarities of DES is that it has the *'complementation property'*: for each plaintext $\mathbf{p}$ and key $\mathbf{k}$ one has $DES(\overline{\mathbf{p}},\overline{\mathbf{k}})=\overline{DES(\mathbf{p},\mathbf{k})}$, where $\overline{\mathbf{a}}$ means that each zero of $\mathbf{a}$ is replaced by a one, and each one by a zero. HELLMAN et al. [10] pointed out that blockciphers with such a complementation property are vulnerable to a chosen plaintext attack twice as fast as exhaustive key search. Although DES was published more than twelve years ago, still no known plaintext attack on DES is known (in the open literature) that is faster than exhaustive key search. In 1976, DIFFIE and HELLMAN [6,7] discussed the possibility of building a 'special purpose machine' by which one could do an exhaustive search on all 2^{56} keys in one day. Such a machine would consist of one million 'DES-chips'. They expected chip-technology to evolve so rapidly, that within ten years (in 1986!) it would be possible to build such a machine for no more than about $20,000,000. It seems that it is not yet possible to build a machine as proposed by Diffie and Hellman for such a low price. But obviously it is possible to construct a cheaper machine that needs more time to search for the key.

To ascertain that a particular blockcipher is secure, one has to find out which weaknesses would make that blockcipher vulnerable to fast known- or chosen plaintext attacks, and to convince one-self that the blockcipher does not have such weaknesses. Dangerous weaknesses are *'bit independencies'*: some of the ciphertext bits are independent of some of the plaintext bits and key bits, i.e. these ciphertext bits can be expressed as functions having only the other plaintext bits and key bits as their arguments. If we denote that subset of ciphertext bits by $B\mathbf{c}$, and the subsets of plaintext bits and key bits on which they depend by $A_1\mathbf{p}$ and $A_2\mathbf{k}$, respectively, then there is a mapping $\tilde{F}$ such that

$$B\mathbf{c} = \tilde{F}(A_1\mathbf{p},A_2\mathbf{k}) \text{ for all } \mathbf{p},\mathbf{k},\mathbf{c} \text{ with } \mathbf{c}=F(\mathbf{p},\mathbf{k}). \tag{1}$$

Hence, the unknown key $\mathbf{k}$ can be computed from a given plaintext $\mathbf{p}$ and a corresponding ciphertext $\mathbf{c}$ by trying all $\tilde{\mathbf{k}}$ in the image of A_2 until one gets $B\mathbf{c}=\tilde{F}(A_1\mathbf{p},\tilde{\mathbf{k}})$ and, after $\tilde{\mathbf{k}}$ has been found, searching exhaustively through all $\mathbf{k}$ with $A_2\mathbf{k}=\tilde{\mathbf{k}}$. This known plaintext attack is much faster than exhaustive key search. MEYER [12] pointed out that truncations of DES that are the iteration of less than five rounds do have bit independencies, and he argued that bit independencies do not appear in blockciphers with at least five rounds of DES; see also the table on p. 265 of [11].

In general, a blockcipher F is also vulnerable to a known plaintext attack much faster than exhaustive key search if it is easy to find any four mappings $\tilde{F}$, A_1, A_2 and B satisfying (1), such that the images under A_1 and A_2 are strings of zeros or ones of length smaller than the message length and key length, respectively, the computation time of $\tilde{F}$ is about the same as that of F,

and the computation times of A_1, A_2 and B are negligible compared with that of F. Such a tuple of mappings $(\tilde{F},A_1,A_2,B)$ is called a *factorization* of F. In general, it is a very complicated problem to find factorizations of a given blockcipher, or to show that there are none. Most of the research that has been done so far restricts itself to *linear* factorizations, i.e. if we consider $\{0,1\}$ as the finite field $\mathbb{F}_2$, and $\{0,1\}^m$ and $\{0,1\}^k$ as vector spaces over $\mathbb{F}_2$, then A_1, A_2 and B (but not necessarily F) are linear mappings on these vectorspaces. To be consistent with the literature, we call the triple (A_1,A_2,B) a *partial linearity* and $\tilde{F}$ a *linear factor* of F, although $\tilde{F}$ itself need not be linear.

REEDS and MANFERDELLI [15] were the first to look for linear factorizations of DES other than bit independencies. They proved that DES has no 'per round linear factors;' roughly speaking this means that DES has no partial linearity that can be composed of the same partial linearities in each round of DES.

CHAUM and EVERTSE [2] extended the notion of a per round linear factor to that of a 'sequence of linear factors,' and proved that DES has no partial linearity caused by such a sequence. Essentially, this means that DES has no partial linearities built up from possibly different partial linearities in the rounds of DES. Chaum and Evertse also analysed blockciphers composed of a reduced number of rounds of DES. They proved that blockciphers with at least five rounds of DES do not have partial linearities caused by sequences of linear factors. This cannot be improved since the bit independencies in DES-truncations of less than five rounds discovered by Meyer come from sequences of linear factors. We remark that no method is known for detecting partial linearities in DES that are not built up from partial linearities in the rounds.

In the present paper, the notion of partial linearity is extended to that of 'linear structures'. Apart from the partial linearities, the class of linear structures contains structures like the complementation property of DES mentioned above. As before, consider $\{0,1\}$ as the field $\mathbb{F}_2$. By $\mathbb{F}_2^m$ we denote the vector space of m-tuples with entries in $\mathbb{F}_2$ and by $+$ vector addition in this space; this vector addition is just coordinatewise addition modulo 2 (otherwise called 'bitwise exclusive-or'). In general, a linear structure of a mapping $S: \mathbb{F}_2^u \to \mathbb{F}_2^v$ is a pair $(\mathcal{V},B)$, where $\mathcal{V}$ is a linear subspace of $\mathbb{F}_2^u$ and B is a linear mapping with domain $\mathbb{F}_2^v$ (both with respect to $\mathbb{F}_2$), such that there is a mapping ψ defined on $\mathcal{V}$ with

$$BS(\mathbf{x}+\mathbf{x}_0) = BS(\mathbf{x})+\psi(\mathbf{x}_0) \text{ for each } \mathbf{x} \text{ in } \mathbb{F}_2^u,\ \mathbf{x}_0 \text{ in } \mathcal{V}. \tag{2}$$

Thus, if $(\mathcal{V},B)$ is a linear structure of a blockcipher with message length m and key length k, then $\mathcal{V}$ is a linear subspace of $\mathbb{F}_2^m \times \mathbb{F}_2^k$ and B is defined on $\mathbb{F}_2^m$. Informally, (2) says that when the input $\mathbf{x}$ is changed by adding some vector in $\mathcal{V}$ to it, then the resulting change in the output $BS(\mathbf{x})$ depends only on the *change* in $\mathbf{x}$, and not on $\mathbf{x}$ itself.

1.2. Contents of the paper

In Section 2 we introduce some notation and mention some preliminary facts about blockciphers.

In Section 3 we explain why blockciphers with linear structures may be vulnerable to known- or chosen plaintext attacks faster than exhaustive key search.

We are particularly interested in linear structures of *product ciphers*. These are blockciphers composed of 'simple' blockciphers ('rounds'). In Section 4 we explain how linear structures of product ciphers can be constructed from linear structures in their rounds; linear structures constructed in this way are said to be *recursive* over the rounds. Recursive linear structures in product ciphers are generalisations of the sequences of linear factors introduced in [2]. In many situations, the linear structures of the rounds, and consequently the recursive linear structures of the product cipher, can be found quite easily; however it is often a hard problem to decide whether a product cipher has a linear structure not recursive over its rounds that enables known- or chosen plaintext attacks faster than exhaustive key search.

In Section 5 we describe DES in more detail, and state Theorem 1: that blockciphers which are the product of at least seven consecutive rounds of DES do not have any recursive linear structure other than the complementation property mentioned above.

In Section 6 we deal with DES-like ciphers. These are product ciphers of a similar structure as DES composed of S-boxes and linear mappings. It is shown that the linear structures of a round of a DES-like cipher can be expressed easily in terms of linear structures of its S-boxes. It is shown that DES-like ciphers have a recursive linear structure analogous to the complementation property of DES. In Section 6 we state and prove Theorem 2: that any DES-like cipher satisfying certain easily verifiable conditions has apart from its complementation property no linear structures that are recursive over its rounds. Further, Theorem 1 is derived from Theorem 2.

In Section 7 we explain briefly that a DES-like cipher might be vulnerable to known- or chosen plaintext attacks faster than exhaustive key search if some of its S-boxes can be changed into S-boxes with linear structures by appropriately changing some of their outputs.

2. Notation and definitions

In this section we introduce some notation to be used in the remainder of this paper, and mention some preliminary facts about linear structures in blockciphers.

When using notions from linear algebra such as vector spaces, linear mappings, etc., it is assumed that the underlying field of scalars is the field of two elements $\mathbb{F}_2$. For every vector space we consider, we denote the addition operation by $+$ and, if confusion is not likely to arise, the zero vector by $\mathbf{0}$. $\mathbb{F}_2^m$ denotes the vector space consisting of all strings of the type $a_1...a_m$ with $a_1,...,a_m \in \mathbb{F}_2$, in which the addition of two strings is just componentwise $\mathbb{F}_2$-addition. Strings in $\mathbb{F}_2^m$ are mostly represented by bold face characters $\mathbf{a}$, $\mathbf{b}$,

etc.; $\mathbf{0}_m$ denotes the string of m zeros and $\mathbf{1}_m$ the string of m ones. Elements of the cartesian product $\mathbb{F}_2^{m_1} \times \ldots \times \mathbb{F}_2^{m_r}$ are denoted by tuples $(\mathbf{x}_1,\ldots,\mathbf{x}_r)$, where $\mathbf{x}_i \in \mathbb{F}_2^{m_i}$ for $i=1,\ldots,r$. We identify the tuple $(\mathbf{x}_1,\ldots,\mathbf{x}_r)$ with the concatenation of the strings represented by $\mathbf{x}_1,\ldots,\mathbf{x}_r$. $[\mathbf{x}]$ denotes the vector space generated by $\mathbf{x}$. If $\mathbb{V}_\alpha$ $(\alpha \in A)$ are (linear) subspaces of the same vector space, then $\bigoplus_{\alpha\in A} \mathbb{V}_\alpha$ $=\{\Sigma_{\alpha\in A} x_\alpha\colon x_\alpha \in \mathbb{V}_\alpha\}$ denotes the smallest vector space containing each $\mathbb{V}_\alpha$. Thus, $\bigoplus_{\alpha\in A}[\mathbf{x}_\alpha]$ denotes the vector space generated by the set of vectors $\{\mathbf{x}_\alpha : \alpha \in A\}$. For any linear mapping A with domain $\mathbb{F}_2^m$ we put $ker(A)=\{\mathbf{x}\in\mathbb{F}_2^m : A\mathbf{x}=\mathbf{0}\}$ and $im(A)=\{A\mathbf{x}:\mathbf{x}\in\mathbb{F}_2^m\}$. A linear mapping is said to be *trivial* if it maps every vector in its domain onto $\mathbf{0}$.

We recall that a *blockcipher* is a mapping

$$F\colon \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$$

(where $\mathbb{F}_2^m$ and $\mathbb{F}_2^k$ are the *message space* and *key space,* respectively) such that for each $\mathbf{k}$ in $\mathbb{F}_2^k$, the mapping

$$F_\mathbf{k} := F(\cdot,\mathbf{k})\colon \mathbb{F}_2^m \to \mathbb{F}_2^m \tag{3}$$

is invertible. The set of blockciphers with message space $\mathbb{F}_2^m$ and key space $\mathbb{F}_2^k$ can be endowed with a group operation. The *product* $F=F_R \cdots F_1$ of the blockciphers $F_1,\ldots,F_R\colon \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$ is defined by

$$F_\mathbf{k}(\mathbf{p}) = F_{R,\mathbf{k}} \cdots F_{1,\mathbf{k}}(\mathbf{p}) \tag{4}$$

(composition of mappings $F_{i,\mathbf{k}}=F_i(.,\mathbf{k})$) for $\mathbf{p}\in\mathbb{F}_2^m$ and $\mathbf{k}\in\mathbb{F}_2^k$. $F_1,\ldots,F_R$ are called the *rounds* of F. The *inverse* F^{-1} of the blockcipher $F\colon \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$ is defined by $F^{-1}(\mathbf{p},\mathbf{k})=\{F_\mathbf{k}\}^{-1}(\mathbf{p})$, where $\{F_\mathbf{k}\}^{-1}$ denotes the inverse of $F_\mathbf{k}$ for each $\mathbf{k}$ in $\mathbb{F}_2^k$.

We recall the following

DEFINITION. A *linear structure* of a blockcipher $F\colon \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$ is a pair $(\mathbb{V},B)$, where $\mathbb{V}$ is a subspace of $\mathbb{F}_2^m \times \mathbb{F}_2^k$ and B is a linear mapping on $\mathbb{F}_2^m$, for which there is a mapping ψ on $\mathbb{V}$ such that

$$BF(\mathbf{p}+\mathbf{p}_0,\ \mathbf{k}+\mathbf{k}_0)+BF(\mathbf{p},\mathbf{k}) = BF(\mathbf{p}_0,\mathbf{k}_0)+BF(\mathbf{0}_m,\mathbf{0}_k) = \psi(\mathbf{p}_0,\ \mathbf{k}_0) \tag{5}$$

for all $(\mathbf{p}_0,\mathbf{k}_0)\in\mathbb{V}$, $\mathbf{p}\in\mathbb{F}_2^m$ and $\mathbf{k}\in\mathbb{F}_2^k$.

A linear structure $(\mathbb{V},B)$ is called *trivial* if either B is trivial or if $\mathbb{V}=[(\mathbf{0}_m,\mathbf{0}_k)]$.

REMARK 1. Every blockcipher has trivial linear structures.

REMARK 2. The mapping ψ in (5) must be linear on $\mathbb{V}$. Indeed, let $(\mathbf{p}_0,\mathbf{k}_0)$, $(\mathbf{p}_1,\mathbf{k}_1)\in\mathbb{V}$. Then (5) implies that

$$\begin{aligned}\psi(\mathbf{p}_0+\mathbf{p}_1,\ \mathbf{k}_0+\mathbf{k}_1) &= BF(\mathbf{p}_1+\mathbf{p}_0,\ \mathbf{k}_1+\mathbf{k}_0)+BF(\mathbf{0}_m,\mathbf{0}_k)\\ &= BF(\mathbf{p}_1+\mathbf{p}_0,\ \mathbf{k}_1+\mathbf{k}_0)+BF(\mathbf{p}_1,\mathbf{k}_1)+BF(\mathbf{p}_1,\mathbf{k}_1)+BF(\mathbf{0}_m,\mathbf{0}_k)\\ &= \psi(\mathbf{p}_0,\ \mathbf{k}_0)+\psi(\mathbf{p}_1,\mathbf{k}_1).\end{aligned}$$

REMARK 3. Let $(\mathcal{V},B)$ be a linear structure of F and put $\mathcal{W}=ker(B)$. It is easy to check that for each pair $(\mathbf{p}_0,\mathbf{k}_0)$ in $\mathcal{V}$, each $\mathbf{p}$ in $\mathbb{F}_2^m$ and each $\mathbf{k}$ in $\mathbb{F}_2^k$ we have

$$F(\mathbf{p}+\mathbf{p}_0,\ \mathbf{k}+\mathbf{k}_0)+F(\mathbf{p},\mathbf{k})+F(\mathbf{p}_0,\mathbf{k}_0)+F(\mathbf{0}_m,\mathbf{0}_k)\ \in\mathcal{W}. \tag{6}$$

On the other hand, if $\mathcal{V}$ and $\mathcal{W}$ are subspaces of $\mathbb{F}_2^m\times\mathbb{F}_2^k$ and $\mathbb{F}_2^m$, respectively, satisfying (6), then each pair $(\mathcal{V},B)$ for which B is a linear mapping on $\mathbb{F}_2^m$ with $ker(B)=\mathcal{W}$ is a linear structure of F.

We now give a few examples of linear structures.

EXAMPLE 1: COMPLEMENTATION PROPERTY OF DES. The blockcipher DES, with message space $\mathbb{F}_2^{64}$ and key space $\mathbb{F}_2^{56}$, has the property that $DES(\mathbf{p}+\mathbf{1}_{64},\ \mathbf{k}+\mathbf{1}_{56})=DES(\mathbf{p},\mathbf{k})+\mathbf{1}_{64}$ for every plaintext $\mathbf{p}$ and key $\mathbf{k}$. Hence if B is the identity, then $([(\mathbf{1}_{64},\mathbf{1}_{56})],B)$ is a linear structure of DES. In (5) we can take for ψ the mapping defined by $\psi(\mathbf{0}_{64},\mathbf{0}_{56})=\mathbf{0}_{64}$ and $\psi(\mathbf{1}_{64},\mathbf{1}_{56})=\mathbf{1}_{64}$.

EXAMPLE 2: PARTIAL LINEARITY. A blockcipher F is said to have partial linearity if there are a triple of linear mappings (A_1,A_2,B) and a mapping $\tilde{F}$ such that $BF(\mathbf{p},\mathbf{k})=\tilde{F}(A_1\mathbf{p},A_2\mathbf{k})$ for all plaintexts $\mathbf{p}$ and keys $\mathbf{k}$. Define $\mathcal{V}=ker(A_1)\times ker(A_2)$; then $(\mathcal{V},B)$ is a linear structure of F. The function ψ in (5) is identically zero.

3. CRYPTANALYTIC SIGNIFICANCE OF LINEAR STRUCTURES

In this section we describe a known- and a chosen plaintext attack, which are both based on the existence of linear structures. In these attacks, the following fact is used:

LEMMA 1. *Let $F\colon \mathbb{F}_2^m\times\mathbb{F}_2^k\to\mathbb{F}_2^m$ be a blockcipher and $(\mathcal{V},B)$ a linear structure of F. Further, let A be a linear mapping on $\mathbb{F}_2^m\times\mathbb{F}_2^k$ with $ker(A)=\mathcal{V}$. Then there exist a linear mapping $C\colon \mathbb{F}_2^m\times\mathbb{F}_2^k\to im(B)$ and a (not necessarily linear) mapping $\tilde{F}\colon im(A)\to im(B)$, both easily computable from F, A and B, such that*

$$BF(\mathbf{p},\mathbf{k})\ =\ \tilde{F}A(\mathbf{p},\mathbf{k})+C(\mathbf{p},\mathbf{k})\ \textit{for all}\ \mathbf{p}\ \textit{in}\ \mathbb{F}_2^m,\ \mathbf{k}\ \textit{in}\ \mathbb{F}_2^k.$$

PROOF. Let ψ be the function on $\mathcal{V}$, defined by (5) in Section 2. It follows from Remark 2 of Section 2 that ψ is linear on $ker(A)$; therefore, it is easy to compute from F, A and B. Let A^* be a pseudo-inverse of A, that is a linear mapping $A^*\colon im(A)\to\mathbb{F}_2^m\times\mathbb{F}_2^k$ such that AA^* is the identity on $im(A)$. Such a pseudo-inverse exists and can be easily computed from A. Let $D\colon \mathbb{F}_2^m\times\mathbb{F}_2^k\to\mathbb{F}_2^m\times\mathbb{F}_2^k$ be the linear mapping defined by $D(\mathbf{p},\mathbf{k})=(\mathbf{p},\mathbf{k})+A^*A(\mathbf{p},\mathbf{k})$. Then $D(\mathbf{p},\mathbf{k})\in ker(A)$ for all $\mathbf{p}\in\mathbb{F}_2^m$ and $\mathbf{k}\in\mathbb{F}_2^k$. Put $\tilde{F}=BFA^*$, $C=\psi D$. Then $\tilde{F}$ and C are well-defined mappings that are easily computable from F, A and B, and C is linear. Let $\mathbf{p}$ and $\mathbf{k}$ be arbitrary elements of $\mathbb{F}_2^m$ and $\mathbb{F}_2^k$, respectively and put $(\mathbf{p}_0,\mathbf{k}_0)=D(\mathbf{p},\mathbf{k})$. Then (5) and the fact that $(\mathbf{p}_0,\mathbf{k}_0)\in ker(A)$ imply that

$$BF(\mathbf{p},\mathbf{k}) = BF(\mathbf{p}+\mathbf{p}_0,\ \mathbf{k}+\mathbf{k}_0)+\psi(\mathbf{p}_0,\mathbf{k}_0) = BFA^*A(\mathbf{p},\ \mathbf{k})+C(\mathbf{p},\mathbf{k})$$
$$= \tilde{F}A(\mathbf{p},\mathbf{k})+C(\mathbf{p},\mathbf{k}).$$

This completes the proof of Lemma 1. □

In what follows, $F\colon \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$ is a blockcipher and $(\mathcal{V},B)$ a non-trivial linear structure of F, and A, C and $\tilde{F}$ are mappings satisfying the conditions of Lemma 1. Define the linear mappings

$$A_1\colon \mathbf{p}\mapsto A(\mathbf{p},\mathbf{0}_k),\ A_2\colon \mathbf{k}\mapsto A(\mathbf{0}_m,\mathbf{k}),$$
$$C_1\colon \mathbf{p}\mapsto C(\mathbf{p},\mathbf{0}_k),\ C_2\colon \mathbf{k}\mapsto C(\mathbf{0}_m,\mathbf{k}).$$

Thus, $A(\mathbf{p},\mathbf{k})=A_1\mathbf{p}+A_2\mathbf{k}$, $C(\mathbf{p},\mathbf{k})=C_1\mathbf{p}+C_2\mathbf{k}$. We describe two attacks: a known plaintext attack, where it is assumed that $0<n:=\dim ker(A_2)\leqslant k$; and a chosen plaintext attack in which $ker(A_2)$ is supposed to have dimension 0.

A known plaintext attack. Suppose that a cryptanalist has a plaintext-ciphertext pair $(\mathbf{p},\mathbf{c})$ and wants to find the secret key $\mathbf{k}$ with $F(\mathbf{p},\mathbf{k})=\mathbf{c}$. In order to find $\mathbf{k}$, he proceeds as follows:

(i) he runs through all values $\tilde{\mathbf{k}}$ in $im(A_2)$ and checks for each $\tilde{\mathbf{k}}$, if the system of linear equations

$$\left.\begin{aligned} A_2\mathbf{k} &= \tilde{\mathbf{k}} \\ C_2\mathbf{k} &= B\mathbf{c}+\tilde{F}(A_1\mathbf{p}+\tilde{\mathbf{k}})+C_1\mathbf{p} \end{aligned}\right\} \quad \text{in } \mathbf{k}\in\mathbb{F}_2^k \tag{7}$$

is soluble (the costs of this are approximately those of a computation of F, if we suppose that F is much more 'complicated' than a linear mapping); it follows at once from Lemma 1 that the unknown key $\mathbf{k}$ must satisfy (7);

(ii) for each $\tilde{\mathbf{k}}$ in $im(A_2)$ for which (7) is soluble, the cryptanalist checks for each solution $\mathbf{k}$ of (7) if $F(\mathbf{p},\mathbf{k})=\mathbf{c}$.

Supposing that our cryptanalist finds L values of $\tilde{\mathbf{k}}$ in (i), and that the null space of the linear mapping $\mathbf{k}\mapsto(A_2\mathbf{k},C_2\mathbf{k})$ has dimension $n_1\leqslant n$, he will find the key after about $2^{k-n}+L\times 2^{n_1}$ encryptions. In general, this number of encryptions is smaller than that needed in exhaustive key search, which is 2^k.

REMARK 1. If the cryptanalist possesses more plaintext-ciphertext pairs for that same key, then he can reduce the number of values L of $\tilde{\mathbf{k}}$ that have to be considered in phase (ii) as follows: whenever the cryptanalist finds a $\tilde{\mathbf{k}}$ for which (7) is soluble, he considers also systems of type (7) with the same $\tilde{\mathbf{k}}$ but with other plaintext-ciphertext pairs instead of $\mathbf{p}$ and $\mathbf{c}$, and checks if all systems under consideration have a common solution; if not, the cryptanalist rejects $\tilde{\mathbf{k}}$. If we assume that our blockcipher is randomly chosen from all blockciphers with linear structure $(\mathcal{V},B)$, then the expected number L of $\tilde{\mathbf{k}}$'s

that have to be considered in phase (ii) decreases in the number of plaintext-ciphertext pairs that the cryptanalist uses; if the number of these pairs is sufficiently large, then the expected value of L drops to 1. This heuristic argument is worked out in more detail in [2], Section 2 for the special case that $(\mathcal{V},B)$ corresponds to a number of bit independencies. Note that in phase (i) the cryptanalist must do some extra work only for those $\tilde{\mathbf{k}}$'s for which (7) is soluble. Thus, the loss in phase (i) is negligible compared with the gain in phase (ii).

REMARK 2. If F^{-1} has a linear structure, then F is vulnerable to a similar known plaintext attack as described above, in which F^{-1} replaces F and $\mathbf{p}$ and $\mathbf{c}$ are interchanged.

REMARK 3. It is possible to use linear structures in 'meet-in-the-middle attacks' as described in [2]. Meet-in-the-middle attacks are known plaintext attacks applicable to product ciphers $F=HG$, where G, $H: \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$ are blockciphers. Suppose that a cryptanalist has a plaintext-ciphertext pair $(\mathbf{p},\mathbf{c})$. Instead of trying to solve the unknown key directly from $\mathbf{c}=F(\mathbf{p},\mathbf{k})$, he could attempt to solve $\mathbf{k}$ from

$$G(\mathbf{p},\mathbf{k}) = H^{-1}(\mathbf{c},\mathbf{k}). \tag{8}$$

It might be advantageous to use (8) if G and H^{-1} have non-trivial linear structures that 'fit' together, whereas the product HG has no non-trivial linear structure. We do not work this out here. CHAUM and EVERTSE [2] discovered that certain product ciphers composed of less than eight rounds of DES are vulnerable to meet-in-the-middle-attacks faster than exhaustive key search.

EXAMPLE 1: PARTIAL LINEARITY. Let A_1,A_2,B be linear mappings such that $BF(\mathbf{p},\mathbf{k})=\tilde{F}(A_1\mathbf{p},A_2\mathbf{k})$ for every plaintext $\mathbf{p}$ and key $\mathbf{k}$, and suppose that $ker(A_2)$ has dimension >0. In [15] and [2] a known plaintext attack based on partial linearity was described that is faster than exhaustive key search. That attack is the same as the attack described above, with C_1 and C_2 being trivial.

A chosen plaintext attack. Suppose that a cryptanalist has N different plaintext-ciphertext pairs, $(\mathbf{p}_1,\mathbf{c}_1),\ldots,(\mathbf{p}_N,\mathbf{c}_N)$, say, and wants to find the unknown key $\mathbf{k}$ for which $F(\mathbf{p}_1,\mathbf{k})=\mathbf{c}_1,\ldots,F(\mathbf{p}_N,\mathbf{k})=\mathbf{c}_N$. Assume that $\mathbf{p}_1,\ldots,\mathbf{p}_N$ have the property that there are $\mathbf{k}_1,\ldots,\mathbf{k}_N \in \mathbb{F}_2^k$ such that

$$A(\mathbf{p}_1,\mathbf{k}_1) = A(\mathbf{p}_2,\mathbf{k}_2) = \cdots = A(\mathbf{p}_N,\mathbf{k}_N). \tag{9}$$

Note that plaintexts $\mathbf{p}_1,\ldots,\mathbf{p}_N$ with this property exist if and only if $\mathcal{V}=ker(A)$ has cardinality at least N. In order to find $\mathbf{k}$, the cryptanalist proceeds as follows: he chooses keys $\mathbf{k}'$ from $\mathbb{F}_2^k$ at random and checks for each $\mathbf{k}'$ if

$$C_2(\mathbf{k}'+\mathbf{k}_1+\mathbf{k}_i) = B\mathbf{c}_i + \tilde{F}A(\mathbf{p}_1,\mathbf{k}') + C_1\mathbf{p}_i \tag{10}$$

holds for some i in $\{1,\ldots,N\}$. If this is the case, the cryptanalist concludes that $\mathbf{k}=\mathbf{k}'+\mathbf{k}_1+\mathbf{k}_i$ must be the proper key. His motivation for this is, that by (9),

(10) and Lemma 1 this $\mathbf{k}$ satisfies

$$B\mathbf{c}_i = \tilde{F}A(\mathbf{p}_i,\mathbf{k})+C(\mathbf{p}_i,\mathbf{k})=BF(\mathbf{p}_i,\mathbf{k}).$$

Thus for the costs of only a single encryption, the cryptanalist can check N keys. Therefore, the expected running time of this attack is about N times smaller than that of exhaustive key search.

REMARK 4. The chosen plaintext attack can also be used when $0<\text{dimension } ker(A_2)\leqslant k$, but in that case its benefit is much less than that of the known plaintext attack described above. However, it is possible to combine both attacks described above into a chosen plaintext attack that is somewhat faster than the known plaintext attack described above.

EXAMPLE 2: COMPLEMENTATION PROPERTY OF DES. HELLMAN et al. ([10], Section III) showed that DES is vulnerable to a chosen plaintext attack, based on the complementation property, which is twice as fast as exhaustive key search. That attack is essentially the chosen plaintext attack described above, applied to DES and two plaintext-ciphertext pairs $(\mathbf{p}_1,\mathbf{c}_1)$, $(\mathbf{p}_2,\mathbf{c}_2)$ with $\mathbf{p}_2=\mathbf{p}_1+\mathbf{1}_{64}$. Note that any two such pairs satisfy (9) with $N=2$, where A is a linear mapping with $ker(A)=[\mathbf{1}_{64},\mathbf{1}_{56}]$, and $\mathbf{k}_1$ and $\mathbf{k}_2$ are any two keys with $\mathbf{k}_2=\mathbf{k}_1+\mathbf{1}_{56}$.

EXAMPLE 3: MULTIPLE COMPLEMENTATION PROPERTIES. Let $f:\mathbb{F}_2^m\to\mathbb{F}_2^m$ be a one-to-one function such that both f and its inverse are easy to compute, and let $F^*:\mathbb{F}_2^m\times\mathbb{F}_2^m\to\mathbb{F}_2^m$ be the blockcipher defined by $F^*(\mathbf{p},\mathbf{k})=f(\mathbf{p}+\mathbf{k})+\mathbf{k}$. Let $\mathcal{V}=\{(\mathbf{p},\mathbf{k})\in\mathbb{F}_2^m\times\mathbb{F}_2^m:\mathbf{p}=\mathbf{k}\}$ and let B be the identity; then $(\mathcal{V},B)$ is a linear structure of F. Lemma 1 holds with $F=f$, $A:(\mathbf{p},\mathbf{k})\mapsto\mathbf{p}+\mathbf{k}$ and $C:(\mathbf{p},\mathbf{k})\mapsto\mathbf{k}$. Any N different plaintexts $\mathbf{p}_1,\ldots,\mathbf{p}_N$ of F^* satisfy condition (9) with $\mathbf{k}_i=\mathbf{p}_i$ for $i=1,\ldots,N$. Hence if a cryptanalist knows N arbitrary plaintext-ciphertext pairs of F^*, corresponding to the same unknown key, then he can find that key about N times faster than with exhaustive search by using the chosen plaintext attack described above. Note that for the blockcipher F^*, this chosen plaintext attack is in fact a *known* plaintext attack.

4. LINEAR STRUCTURES IN PRODUCT CIPHERS

Let $F_1,\ldots,F_R:\mathbb{F}_2^m\times\mathbb{F}_2^k\to\mathbb{F}_2^m$ be blockciphers, and let $F=F_R\cdots F_1$ be their product. We describe how linear structures of F can be constructed from linear structures in $F_1,\ldots,F_R$. To this end, we introduce the so-called T-spaces and U-spaces.

For any blockcipher $F:\mathbb{F}_2^m\times\mathbb{F}_2^k\to\mathbb{F}_2^m$, and any subspace $\mathcal{V}$ of $\mathbb{F}_2^m\times\mathbb{F}_2^k$, we define the spaces

$$T(F,\mathcal{V}) = \bigoplus_{(\mathbf{p}_0,\mathbf{k}_0)\in\mathcal{V}} \bigoplus_{(\mathbf{p},\mathbf{k})\in\mathbb{F}_2^m\times\mathbb{F}_2^k} [(F(\mathbf{p}+\mathbf{p}_0,\ \mathbf{k}+\mathbf{k}_0)+F(\mathbf{p},\mathbf{k}),\mathbf{k}_0)],$$

$$U(F,\mathcal{V}) = \bigoplus_{\substack{(\mathbf{p}_0,\mathbf{k}_0)\in\mathcal{V}\\(\mathbf{p},\mathbf{k})\in\mathbb{F}_2^m\times\mathbb{F}_2^k}} [F(\mathbf{p}+\mathbf{p}_0,\ \mathbf{k}+\mathbf{k}_0)+F(\mathbf{p},\mathbf{k})+F(\mathbf{p}_0,\mathbf{k}_0)+F(\mathbf{0}_m,\mathbf{0}_k)].$$

Thus $T(F,\mathcal{V}) \subseteq \mathbb{F}_2^m \times \mathbb{F}_2^k$, $U(F,\mathcal{V}) \subseteq \mathbb{F}_2^m$, and $U(F,\mathcal{V}) \times [\mathbf{0}_k] \subseteq T(F,\mathcal{V})$. In view of Remark 3 of Section 2 we have

$$(\mathcal{V},B) \text{ linear structure of } F \Leftrightarrow U(F,\mathcal{V}) \subseteq ker(B). \tag{11}$$

In other words, $U(F,\mathcal{V})$ is the minimal space that is the null space of a linear mapping B for which $(\mathcal{V},B)$ is a linear structure of F.

Unfortunately, it is not possible to construct linear structures in the product cipher directly from the U-spaces of its rounds; in our construction we also need the T-spaces. However, T-spaces can be computed easily once the U-spaces are known, as is shown below.

LEMMA 2. *Let* $F: \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$ *be a blockcipher and* $\mathcal{V} = \oplus_{i=1}^{s} [(\mathbf{p}_i, \mathbf{k}_i)]$ *a subspace of* $\mathbb{F}_2^m \times \mathbb{F}_2^k$. *Then*

$$T(F,\mathcal{V}) = \{U(F,\mathcal{V}) \times [\mathbf{0}_k]\} \oplus \{\bigoplus_{i=1}^{s} [(F(\mathbf{p}_i,\mathbf{k}_i) + F(\mathbf{0}_m,\mathbf{0}_k),\mathbf{k}_i)]\}. \tag{12}$$

PROOF. Denote the space at the right-hand side of (12) by $\mathcal{X}$. It is easy to check that $\mathcal{X} \subseteq T(F,\mathcal{V})$. In order to prove that $T(F,\mathcal{V}) \subseteq \mathcal{X}$, it suffices to show that for each $(\mathbf{p}_0,\mathbf{k}_0)$ in $\mathcal{V}$, $\mathbf{p}$ in $\mathbb{F}_2^m$ and $\mathbf{k}$ in $\mathbb{F}_2^k$ we have

$$(F(\mathbf{p}+\mathbf{p}_0,\ \mathbf{k}+\mathbf{k}_0) + F(\mathbf{p},\mathbf{k}),\mathbf{k}_0) \in \mathcal{X}. \tag{13}$$

Without loss of generality we may assume that $(\mathbf{p}_0,\mathbf{k}_0) = \Sigma_{i=1}^{t} (\mathbf{p}_i,\mathbf{k}_i)$, where $1 \leqslant t \leqslant s$. Then

$$(F(\mathbf{p}+\mathbf{p}_0,\ \mathbf{k}+\mathbf{k}_0) + F(\mathbf{p},\mathbf{k}),\mathbf{k}_0) = \sum_{i=1}^{t} \mathbf{a}_i,$$

where $\mathbf{a}_1 = (F(\mathbf{p}+\mathbf{p}_1,\ \mathbf{k}+\mathbf{k}_1) + F(\mathbf{p},\mathbf{k}),\mathbf{k}_1)$ and

$$\mathbf{a}_i = \left[F(\mathbf{p} + \sum_{j=1}^{i} \mathbf{p}_j, \mathbf{k} + \sum_{j=1}^{i} \mathbf{k}_j) + F(\mathbf{p} + \sum_{j=1}^{i-1} \mathbf{p}_j, \mathbf{k} + \sum_{j=1}^{i-1} \mathbf{k}_j), \mathbf{k}_i \right]$$

for $i = 2,\ldots,t$. It is easy to check that for each i, $\mathbf{a}_i + (F(\mathbf{p}_i,\mathbf{k}_i) + F(\mathbf{0}_m,\mathbf{0}_k),\mathbf{k}_i)$ belongs to $U(F,\mathcal{V}) \times [\mathbf{0}_k]$. This proves Lemma 2. □

The next, rather technical, lemma shows how T-spaces and U-spaces of the rounds can be used to construct linear structures of the product cipher, provided that these T-spaces and U-spaces satisfy some recurrence relation.

LEMMA 3. *Let* $F_1,\ldots,F_R: \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$ *be blockciphers and put* $F = F_R \cdots F_1$. *Suppose that* $\mathcal{V}_0$, $\mathcal{V}_1,\ldots,\mathcal{V}_R$ *are subspaces of* $\mathbb{F}_2^m \times \mathbb{F}_2^k$, *and* $\mathcal{W}_0$, $\mathcal{W}_1,\ldots,\mathcal{W}_R$ *are subspaces of* $\mathbb{F}_2^m$, *such that*

$$\left.\begin{aligned} \mathcal{V}_i &\supseteq T(F_i,\mathcal{V}_{i-1}), \\ \mathcal{W}_i \times [\mathbf{0}_k] &\supseteq T(F_i,\mathcal{W}_{i-1} \times [\mathbf{0}_k]) \oplus \{U(F_i,\mathcal{V}_{i-1}) \times [\mathbf{0}_k]\} \text{ for } i = 1,\ldots,R. \end{aligned}\right\} \tag{14}$$

Then $U(F,\mathcal{V}_0) \subseteq \mathcal{W}_R$.

(11) and Lemma 3 motivate the following:

DEFINITION. Let $F_1,\ldots,F_R: \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$ be blockciphers and put $F = F_R \cdots F_1$. A linear structure $(\mathcal{V},B)$ of F is called *recursive* over $F_1,\ldots,F_R$ if there are subspaces $\mathcal{V}_0,\ldots,\mathcal{V}_R$ of $\mathbb{F}_2^m \times \mathbb{F}_2^k$ and $\mathcal{W}_0,\ldots,\mathcal{W}_R$ of $\mathbb{F}_2^m$ for which (14) holds and for which $\mathcal{V}=\mathcal{V}_0$ and $ker(B)=\mathcal{W}_R$.

REMARK 1. If a product cipher can be decomposed into rounds in two different ways, then it is possible that a linear structure of that product cipher is recursive over the rounds of the first decomposition but not over the rounds of the second decomposition.

REMARK 2. If the rounds of some product cipher are such that their linear structures are easy to find, then in general, the linear structures of that product cipher which are recursive over its rounds are also easy to detect. However, one cannot exclude that a product cipher has linear structures that are *not* recursive over its rounds, and it might be a very difficult problem to find out if such non-recursive linear structures exist.

PROOF OF LEMMA 3. In the proof of Lemma 3 we need the following facts: for any two blockciphers $G, H: \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$ we have

$$T(HG,\mathcal{V}) \subseteq T(H,T(G,\mathcal{V})) \tag{15}$$

and

$$U(HG,\mathcal{V})\times[\mathbf{0}_k] \subseteq T(H,U(G,\mathcal{V})\times[\mathbf{0}_k])\oplus\{U(H,T(G,\mathcal{V}))\times[\mathbf{0}_k]\}. \tag{16}$$

We first prove (15). Let $\mathbf{p}\in\mathbb{F}_2^m$, $\mathbf{k}\in\mathbb{F}_2^k$ and $(\mathbf{p}_0, \mathbf{k}_0)\in\mathcal{V}$, and put $\mathbf{p}_1 = G(\mathbf{p},\mathbf{k})$, $\tilde{\mathbf{p}}_0 = G(\mathbf{p}+\mathbf{p}_0, \mathbf{k}+\mathbf{k}_0)+G(\mathbf{p},\mathbf{k})$. Then

$$(HG(\mathbf{p}+\mathbf{p}_0, \mathbf{k}+\mathbf{k}_0)+HG(\mathbf{p},\mathbf{k}),\mathbf{k}_0) =$$

$$H(\mathbf{p}_1+\tilde{\mathbf{p}}_0, \mathbf{k}+\mathbf{k}_0)+H(\mathbf{p}_1,\mathbf{k}), \mathbf{k}_0)\in T(H,T(G,\mathcal{V})).$$

This proves (15).

We now prove (16). Put $\mathbf{q}_1 = G(\mathbf{p}+\mathbf{p}_0, \mathbf{k}+\mathbf{k}_0) + G(\mathbf{p},\mathbf{k}) + G(\mathbf{p}_0,\mathbf{k}_0) + G(\mathbf{0}_m,\mathbf{0}_k)$, $\mathbf{q}_2 = G(\mathbf{p}_0,\mathbf{k}_0)+G(\mathbf{0}_m,\mathbf{0}_k)$, $\mathbf{p}_1 = G(\mathbf{p},\mathbf{k})$ and $\mathbf{p}_2 = G(\mathbf{p}_0,\mathbf{k}_0)$. Then $\mathbf{q}_1 \in U(G,\mathcal{V})$ and $(\mathbf{q}_2,\mathbf{k}_0)\in T(G,\mathcal{V})$. Further,

$$HG(\mathbf{p}+\mathbf{p}_0, \mathbf{k}+\mathbf{k}_0)+HG(\mathbf{p},\mathbf{k})+HG(\mathbf{p}_0,\mathbf{k}_0)+HG(\mathbf{0}_m,\mathbf{0}_k) = \mathbf{a}+\mathbf{b}+\mathbf{c},$$

where

$$\mathbf{a} = H(\mathbf{p}_1+\mathbf{q}_2+\mathbf{q}_1, \mathbf{k}+\mathbf{k}_0)+H(\mathbf{p}_1+\mathbf{q}_2, \mathbf{k}+\mathbf{k}_0) \text{ and } (\mathbf{a},\mathbf{0}_k)\in T(H,U(G,\mathcal{V})\times[\mathbf{0}_k]),$$

$$\mathbf{b} = H(\mathbf{p}_1+\mathbf{q}_2, \mathbf{k}+\mathbf{k}_0)+H(\mathbf{p}_1,\mathbf{k})+H(\mathbf{q}_2,\mathbf{k}_0)+H(\mathbf{0}_m,\mathbf{0}_k)\in U(H,T(G,\mathcal{V})),$$

$$\mathbf{c} = H(\mathbf{p}_2+\mathbf{q}_2,\mathbf{k}_0+\mathbf{k}_0)+H(\mathbf{p}_2,\mathbf{k}_0)+H(\mathbf{q}_2,\mathbf{k}_0)+H(\mathbf{0}_m,\mathbf{0}_k)\in U(H,T(G,\mathcal{V})).$$

This proves (16).

Let $F^{(i)} = F_i \cdots F_1$ for $i = 1,\ldots,R$. We prove by induction on i that

$$\mathcal{V}_i \supseteq T(F^{(i)}, \mathcal{V}_0), \quad \mathcal{W}_i \supseteq U(F^{(i)}, \mathcal{V}_0) \text{ for } i = 1, \ldots, R, \tag{17}$$

which is obviously sufficient. (17) is trivially true for $i = 1$. Suppose that (17) holds for $i = t-1$ (induction hypothesis). In the induction step, we apply (15) and (16) with $G = F^{(t-1)}$, $H = F_t$ and $\mathcal{V} = \mathcal{V}_0$. First we have, by (14), the induction hypothesis and (15), that

$$\mathcal{V}_t \supseteq T(F_t, \mathcal{V}_{t-1}) \supseteq T(F_t, T(F^{(t-1)}, \mathcal{V}_0)) \supseteq T(F^{(t)}, \mathcal{V}_0),$$

and second it follows from (14), the induction hypothesis and (16), that

$$\begin{aligned} \mathcal{W}_t \times [\mathbf{0}_k] &\supseteq T(F_t, \mathcal{W}_{t-1} \times [\mathbf{0}_k]) \oplus \{U(F_t, \mathcal{V}_{t-1}) \times [\mathbf{0}_k]\} \\ &\supseteq T(F_t, U(F^{(t-1)}, \mathcal{V}_0) \times [\mathbf{0}_k]) \oplus \{U(F_t, T(F^{(t-1)}, \mathcal{V}_0)) \times [\mathbf{0}_k]\} \\ &\supseteq U(F^{(t)}, \mathcal{V}_0) \times [\mathbf{0}_k]. \end{aligned}$$

Hence (17) holds for $i = t$. This completes the induction step. □

EXAMPLE. Let $F_1, \ldots, F_R : \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$ be blockciphers and $F = F_R \cdots F_1$. A *sequence of linear factors* for F, as introduced in [2], is a tuple of linear mappings $(C_0, C_1, \ldots, C_R, D)$ such that $C_0, \ldots, C_R$ have domain $\mathbb{F}_2^m$, D has domain $\mathbb{F}_2^k$, and there are mappings $\tilde{F}_1, \ldots, \tilde{F}_R$ with

$$C_i F_i(\mathbf{p}, \mathbf{k}) = \tilde{F}_i(C_{i-1}\mathbf{p}, D\mathbf{k}) \text{ for } i = 1, \ldots, R, \ \mathbf{p} \in \mathbb{F}_2^m, \ \mathbf{k} \in \mathbb{F}_2^k.$$

It is easy to check that the spaces $\mathcal{V}_i = ker(C_i) \times ker(D)$ and $\mathcal{W}_i = ker(C_i)$ $(i = 0, \ldots, R)$ satisfy (14). Hence if $\mathcal{V} = ker(C_0) \times ker(D)$ and $B = C_R$, then $(\mathcal{V}, B)$ is a linear structure of F that is recursive over $F_1, \ldots, F_R$.

5. LINEAR STRUCTURES IN DES

In this section we first give a rough description of the NBS-version of DES. Then we modify DES into a form that can be analysed more conveniently, and describe the recursive linear structures of the modified DES. For each function $\sigma: \{1, \ldots, v\} \to \{1, \ldots, u\}$, we define the *bitmap* $P_\sigma : \mathbb{F}_2^u \to \mathbb{F}_2^v$ by $P(x_1 \cdots x_u) = x_{\sigma(1)} \cdots x_{\sigma(v)}$ for $x_1 \cdots x_u \in \mathbb{F}_2^u$. DES is built up from the bitmaps

$IP = P_{\sigma_1} : \mathbb{F}_2^{64} \to \mathbb{F}_2^{64}$, where σ_1 is a permutation on $\{1, \ldots, 64\}$;

$P = P_{\sigma_2} : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$, where σ_2 is a permutation on $\{1, \ldots, 32\}$;

$E = P_{\sigma_3} : \mathbb{F}_2^{32} \to \mathbb{F}_2^{48}$, where $\sigma_3 : \{1, \ldots, 48\} \to \{1, \ldots, 32\}$ has the property that sixteen integers among $1, \ldots, 32$ have two co-images, while the other sixteen have only one co-image;

$PC1 = P_{\sigma_4} : \mathbb{F}_2^{64} \to \mathbb{F}_2^{56}$, where σ_4 is injective;

$PC2 = P_{\sigma_5} : \mathbb{F}_2^{56} \to \mathbb{F}_2^{48}$, where σ_5 is an injective function that maps $\{1, \ldots, 24\}$ into $\{1, \ldots, 28\}$ and $\{25, \ldots, 48\}$ into $\{29, \ldots, 56\}$;

$C = P_{\sigma_6}: \mathbb{F}_2^{56} \to \mathbb{F}_2^{56}$, where σ_6 is the permutation given by the product of two

28-cycles $(1,2,\ldots,27,28)(29,30,\ldots,55,56)$;

and from the so-called S-boxes $S_1,\ldots,S_8: \mathbb{F}_2^6 \to \mathbb{F}_2^4$. Each S-box S_j is constructed in such a way that for any fixed values of the first and the sixth input bit, S_j acts as a permutation on the set of sixteen combinations of the remaining four input bits. For the precise definitions of $\sigma_1,\ldots,\sigma_6$ and the S-boxes we refer to [13]. Define $S: \mathbb{F}_2^{48} \to \mathbb{F}_2^{32}$ by $S(\mathbf{x}_1,\ldots,\mathbf{x}_8)=(S_1\mathbf{x}_1,\ldots,S_8\mathbf{x}_8)$. In what follows, elements of $\mathbb{F}_2^{64}$ are denoted as pairs $(\mathbf{p},\mathbf{q})$ with $\mathbf{p},\mathbf{q}\in\mathbb{F}_2^{32}$.

In [13], DES is described as a blockcipher with both message length and key length 64; however, only 56 bits of the key are used. We now describe DES according to [13]. Let $\mathbf{p}\in\mathbb{F}_2^{64}$, $\mathbf{k}\in\mathbb{F}_2^{64}$, put $\mathbf{k}'=PC1(\mathbf{k})$ and define $\mathbf{x}_0,\ldots,\mathbf{x}_{17}\in\mathbb{F}_2^{32}$ recursively by

$$IP(\mathbf{p}) = (\mathbf{x}_0,\mathbf{x}_1),$$

$$\mathbf{x}_{i+1} = \mathbf{x}_{i-1}+P\circ S\{E\mathbf{x}_i+PC2\circ C^{k(i)}(\mathbf{k}')\} \text{ for } i=1,\ldots,16;$$

here $\omega(1),\ldots,\omega(16)$ is an increasing sequence of integers. Then the ciphertext $\mathbf{c}=$ DES $(\mathbf{p},\mathbf{k})$ is given by

$$\mathbf{c} = IP^{-1}(\mathbf{x}_{17},\mathbf{x}_{16}).$$

It is easy to see that DES^{-1} is the same as DES, except that the recurrence is applied in the reverse order; hence we get DES^{-1} by replacing $\omega(i)$ by $\omega(17-i)$ in the above description. Note that the ciphertext depends only on the 56-bit key $PC1(\mathbf{k})$. Further, it seems that the mappings IP and $PC1$ do not contribute anything to the strength of DES.

We now describe a slightly modified version of DES. Let $\lambda: \{1,\ldots,32\}\to\{1,\ldots,48\}$ be the function for which $E\circ P=P_\lambda$, and define the function $\delta: \{1,\ldots,48\}\to\{1,\ldots,56\}$ by $\delta(i)=i$ for $1\leqslant i\leqslant 24$ and $\delta(i)=i+4$ for $25\leqslant i\leqslant 48$. Note that $25,\ldots,28$ and $53,\ldots,56$ are not contained in the range of δ. There exists a permutation α on $\{1,\ldots,56\}$ such that α permutes $1,\ldots,28$ and $29,\ldots,56$ and $PC2=P_{\delta\alpha}$. Define the permutation κ on $\{1,\ldots,56\}$ by $P_\kappa=P_\alpha\circ C\circ P_\alpha^{-1}$. Then κ is the product of two cyclic permutations on $\{1,\ldots,28\}$ and $\{29,\ldots,56\}$, respectively. Thus, for each integer i we have $PC2\circ C^i=P_{\delta\kappa^i\alpha}$. In the sequel, elements of $\mathbb{F}_2^{64}$ are denoted by pairs $(\mathbf{p},\mathbf{q})$ with $\mathbf{p},\mathbf{q}\in\mathbb{F}_2^{32}$. For $i=1,\ldots,16$ we define the blockcipher $F_i: \mathbb{F}_2^{64}\times\mathbb{F}_2^{56}\to\mathbb{F}_2^{64}$ by

$$F_i(\mathbf{p},\mathbf{q},\mathbf{k}) = (\mathbf{q},\ \mathbf{p}+S(P_\lambda\mathbf{q}+P_{\delta\kappa^{\omega(i)}}\mathbf{k})).$$

For any pair of integers S,T with $1\leqslant S\leqslant T\leqslant 16$ we put

$$DES_{ST} = F_T\cdots F_S.$$

DES_{ST} can be considered as the composition of rounds S up to T of DES. Defining the map θ on $\mathbb{F}_2^{64}$ by $\theta(\mathbf{p},\mathbf{q})=(\mathbf{q},\mathbf{p})$, we infer that $F_i^{-1}(\mathbf{p},\mathbf{q},\mathbf{k}) = \theta F_i(\mathbf{q},\mathbf{p},\mathbf{k})$ for each i. Therefore

$$DES_{ST}^{-1}(\mathbf{p},\mathbf{q},\mathbf{k}) = \theta\{F_S\cdots F_T(\mathbf{q},\mathbf{p},\mathbf{k})\}.$$

The NBS-version of DES in [13] is expressed in terms of $DES_{1,16}$ by

$$\mathrm{DES}(\mathbf{p},\mathbf{q},\mathbf{k}) = IP^{-1} \circ P \circ \theta DES_{1,16}\{P^{-1} \circ IP(\mathbf{p},\mathbf{q}),\ P_\alpha \circ PC1(\mathbf{k})\}.$$

Each F_i has the complementation property: $F_i((\mathbf{p},\mathbf{q})+\mathbf{1}_{64},\ \mathbf{k}+\mathbf{1}_{56}) = F_i((\mathbf{p},\mathbf{q}),\mathbf{k})+\mathbf{1}_{64}$ for all $\mathbf{p}\in\mathbb{F}_2^{64}$, $\mathbf{k}\in\mathbb{F}_2^{56}$. Hence if $\mathcal{V} = [(\mathbf{1}_{64},\mathbf{1}_{56})]$ and B is the identity, then $(\mathcal{V},B)$ is a linear structure of F_i. It is easy to see that $(\mathcal{V},B)$ is also a linear structure of each blockcipher DES_{ST}, and that this linear structure is recursive over $F_S,\ldots,F_T$. The complementation property is also a recursive linear structure of the inverse blockciphers DES_{ST}^{-1}.

Blockciphers composed of at most six consecutive rounds of DES might have recursive linear structures other than the complementation property. For instance, $DES_{2,7}$ has the property that for each plaintext $\mathbf{p} = p_1p_2\ldots p_{64}$, key $\mathbf{k} = k_1\ldots k_{56}$, and corresponding ciphertext $\mathbf{c}=DES_{2,7}(\mathbf{p},\mathbf{k})=c_1\ldots c_{64}$ (with $p_i,\ k_i,\ c_i\in\mathbb{F}_2$), a simultaneous change of p_{31} and k_4 does not affect the eight bits $c_5,c_6,c_7,c_8,c_{13},c_{14},c_{15},c_{16}$ of $\mathbf{c}$. The next theorem states that product ciphers, consisting of seven or more consecutive rounds of DES, do not have any non-trivial recursive linear structure other than the complementation property.

THEOREM 1. *Let S, T be integers with $1\leqslant S<T\leqslant 16$ and $T\geqslant S+6$, and let $\mathcal{V}$ be a subspace of $\mathbb{F}_2^{64}\times\mathbb{F}_2^{56}$ that is not equal to $[(\mathbf{0}_{64},\mathbf{0}_{56})]$ or $[(\mathbf{1}_{64},\mathbf{1}_{56})]$. If $(\mathcal{V},B)$ is a linear structure of DES_{ST} that is recursive over $F_S,\ldots,F_T$, or if $(\mathcal{V},B)$ is a linear structure of DES_{ST}^{-1} that is recursive over $F_T^{-1},\ldots,F_S^{-1}$, then B is trivial.*

In the next section, we shall derive Theorem 1 from a more general result on 'DES-like' ciphers.

6. LINEAR STRUCTURES IN DES-LIKE CIPHERS

In this section we introduce DES-like ciphers, which are product ciphers with a similar structure as DES. We investigate the recursive linear structures of these DES-like ciphers. The class of DES-like ciphers contains, among others, the blockciphers DES_{ST} introduced in the previous section.

Let m,k,l,n,m_1,n_1,R be positive integers with $m=2lm_1$ and $n=ln_1$. Elements of $\mathbb{F}_2^m$ are often denoted by $(\mathbf{p},\mathbf{q})$, where $\mathbf{p},\mathbf{q}\in\mathbb{F}_2^{\frac{1}{2}m}$. Whenever convenient, we write elements of $\mathbb{F}_2^{\frac{1}{2}m}$ as $(\mathbf{q}_1,\ldots,\mathbf{q}_l)$ with $\mathbf{q}_j\in\mathbb{F}_2^{m_1}$ for $j=1,\ldots,l$ and elements of $\mathbb{F}_2^n$ as l-tuples of elements of $\mathbb{F}_2^{n_1}$. A DES-like cipher with message space $\mathbb{F}_2^m$ and key space $\mathbb{F}_2^k$ is a product cipher

$$F = F_RF_{R-1}\cdots F_1, \tag{18}$$

whose rounds $F_i (i=1,\ldots,R)$ are defined by

$$F_i(\mathbf{p},\mathbf{q},\mathbf{k}) = (\mathbf{q},\ \mathbf{p}+S(L\mathbf{q}+K_i\mathbf{k})) \text{ for } (\mathbf{p},\mathbf{q})\in\mathbb{F}_2^m,\ \mathbf{k}\in\mathbb{F}_2^k. \tag{19}$$

Here the mapping $S:\mathbb{F}_2^n\to\mathbb{F}_2^{\frac{1}{2}m}$ is given by

$$S(\mathbf{x}_1,\ldots,\mathbf{x}_l) = (S_1\mathbf{x}_1,\ldots,S_l\mathbf{x}_l) \text{ for } \mathbf{x}_1,\ldots,\mathbf{x}_l\in\mathbb{F}_2^{n_1},$$

where $S_1,\ldots,S_l:\mathbb{F}_2^{n_1}\to\mathbb{F}_2^{m_1}$ are certain non-linear mappings (the S-boxes);

$L: \mathbb{F}_2^{\frac{1}{2}m} \to \mathbb{F}_2^n$ is a linear mapping; and $K_1,\ldots,K_R: \mathbb{F}_2^k \to \mathbb{F}_2^n$ are linear mappings such that for $i=1,\ldots,R$, the linear mapping $J_i: \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^n$, given by

$$J_i(\mathbf{p},\mathbf{q},\mathbf{k}) = L\mathbf{q} + K_i\mathbf{k},$$

is surjective. We have $F_i^{-1}(\mathbf{p},\mathbf{q},\mathbf{k}) = \theta F_i(\mathbf{q},\mathbf{p},\mathbf{k})$ for each i, where θ is defined on $\mathbb{F}_2^m$ by $\theta(\mathbf{p},\mathbf{q}) = (\mathbf{q},\mathbf{p})$. Hence

$$F^{-1}(\mathbf{p},\mathbf{q},\mathbf{k}) = \theta\{F_1 \cdots F_R(\mathbf{q},\mathbf{p},\mathbf{k})\}.$$

Therefore inverses of DES-like ciphers are also DES-like ciphers, except that the two halves of the plaintext and ciphertext have to be interchanged.

Linear structures in the rounds F_i can be described in terms of linear structures in the S-boxes. We remark that searching for the linear structures in the S-boxes is feasible when the input size n_1 of the S-boxes is small. In that case it is also feasible to find the linear structures in the rounds. For each j in $\{1,\ldots,l\}$ and each subspace $\mathfrak{U}$ of $\mathbb{F}_2^{n_1}$ we define the subspace of $\mathbb{F}_2^{m_1}$

$$U(S_j,\mathfrak{U}) = \bigoplus_{\substack{\mathbf{x}\in\mathbb{F}_2^{n_1} \\ \mathbf{u}\in\mathfrak{U}}} [S_j(\mathbf{x}+\mathbf{u}) + S_j(\mathbf{x}) + S_j(\mathbf{u}) + S_j(\mathbf{0}_{n_1})].$$

Similarly as in Remark 3 of Section 2, it follows that any pair $(\mathfrak{U},B)$, where $\mathfrak{U}$ is a subspace of $\mathbb{F}_2^{n_1}$ and B is a linear mapping on $\mathbb{F}_2^{m_1}$, is a linear structure of S_j if and only if $U(S_j,\mathfrak{U}) \subseteq ker(B)$; $(\mathfrak{U},B)$ is said to be *trivial* if $\mathfrak{U}=[\mathbf{0}_{n_1}]$ or if B is trivial.

Let $\rho_j: \mathbb{F}_2^n \to \mathbb{F}_2^{n_1}$ be the j-th projection given by $\rho_j(\mathbf{x}_1,\ldots,\mathbf{x}_l)=\mathbf{x}_j$. If $(\mathbf{p},\mathbf{q},\mathbf{k}) \in \mathbb{F}_2^m \times \mathbb{F}_2^k$ is an input to some round F_i then $\rho_j J_i(\mathbf{p},\mathbf{q},\mathbf{k})$ is the part of that input going into S-box S_j. In the lemma below, elements of $\mathbb{F}_2^m$ are written as $(\mathbf{p},\mathbf{q}_1,\ldots,\mathbf{q}_l)$, with $\mathbf{p}\in\mathbb{F}_2^{\frac{1}{2}m}$ and $\mathbf{q}_1,\ldots,\mathbf{q}_l \in \mathbb{F}_2^{m_1}$.

LEMMA 4. *Let $i\in\{1,\ldots,R\}$, and suppose that F_i is given by (19). Further, let $\mathfrak{V}$ be a subspace of $\mathbb{F}_2^m \times \mathbb{F}_2^k$. Then*

$$U(F_i,\mathfrak{V}) = [\mathbf{0}_{\frac{1}{2}m}] \times \{U(S_1,\rho_1 J_i(\mathfrak{V})) \times U(S_2,\rho_2 J_i(\mathfrak{V})) \times \cdots \times U(S_l,\rho_l J_i(\mathfrak{V}))\}. \quad (20)$$

PROOF. Denote the space on the right-hand side of (20) by $\mathfrak{L}$. We first prove that $U(F_i,\mathfrak{V}) \subseteq \mathfrak{L}$. To this end, it is sufficient to prove that each vector $F_i(\mathbf{p}+\mathbf{p}_0,\ \mathbf{q}+\mathbf{q}_0,\ \mathbf{k}+\mathbf{k}_0) + F_i(\mathbf{p},\mathbf{q},\mathbf{k}) + F_i(\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0) + F_i(\mathbf{0}_{\frac{1}{2}m},\mathbf{0}_{\frac{1}{2}m},\mathbf{0}_k)$ with $(\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0)\in\mathfrak{V}$ and $(\mathbf{p},\mathbf{q},\mathbf{k})\in\mathbb{F}_2^m\times\mathbb{F}_2^k$ can be written as $(\mathbf{0}_{\frac{1}{2}m},\mathbf{s}_1,\ldots,\mathbf{s}_l)$, where $\mathbf{s}_j \in U(S_j,\rho_j J_i(\mathfrak{V}))$ for $j=1,\ldots,l$. But this follows at once from the definition of F_i and the fact that $S(\mathbf{x})=(S_1\rho_1(\mathbf{x}),\ldots,S_l\rho_l(\mathbf{x}))$: we have

$$\begin{aligned} &F_i(\mathbf{p}+\mathbf{p}_0,\ \mathbf{q}+\mathbf{q}_0,\ \mathbf{k}+\mathbf{k}_0) + F_i(\mathbf{p},\mathbf{q},\mathbf{k}) + F_i(\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0) + F_i(\mathbf{0}_{\frac{1}{2}m},\mathbf{0}_{\frac{1}{2}m},\mathbf{0}_k) \qquad (21)\\ &= (\mathbf{0}_{\frac{1}{2}m}, SJ_i(\mathbf{p}+\mathbf{p}_0,\ \mathbf{q}+\mathbf{q}_0,\ \mathbf{k}+\mathbf{k}_0) + SJ_i(\mathbf{p},\mathbf{q},\mathbf{k}) + SJ_i(\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0) + SJ_i(\mathbf{0}_n))\\ &= (\mathbf{0}_{\frac{1}{2}m}, \mathbf{s}_1, \ldots, \mathbf{s}_l), \end{aligned}$$

where

$$\begin{aligned}\mathbf{s}_j &= S_j(\rho_j J_i(\mathbf{p},\mathbf{q},\mathbf{k})+\rho_j J_i(\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0))+S_j\rho_j J_i(\mathbf{p},\mathbf{q},\mathbf{k})+S_j\rho_j J_i(\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0)+S_j(\mathbf{0}_{n_1})\\ &\in U(S_j,\rho_j J_i(\mathcal{V}))\end{aligned}$$

for $j=1,\ldots,l$.

We now prove that $\mathcal{Z}\subseteq U(F_i,\mathcal{V})$. It obviously suffices to prove that for each t in $\{1,\ldots,l\}$ we have

$$U(F_i,\mathcal{V})\supseteq[\mathbf{0}_{\frac{1}{2}m}]\times([\mathbf{0}_{m_1}]\times\cdots\times U(S_t,\rho_t J_i(\mathcal{V}))\times\cdots\times[\mathbf{0}_{m_1}]), \quad (22)$$

where the space $U(S_t,\rho_t J_i(\mathcal{V}))$ is preceded by $t-1$ spaces $[\mathbf{0}_{m_1}]$ and followed by $l-t$ spaces $[\mathbf{0}_{m_1}]$. In order to prove (22), it is sufficient to show that for each t in $\{1,\ldots,l\}$, $\mathbf{u}$ in $\rho_t J_i(\mathcal{V})$ and $\mathbf{x}$ in $\mathbb{F}_2^{n_1}$, $U(F_i,\mathcal{V})$ contains $(\mathbf{0}_{\frac{1}{2}m},\mathbf{y}_1,\ldots,\mathbf{y}_l)$, where $\mathbf{y}_t = S_t(\mathbf{x}+\mathbf{u})+S_t(\mathbf{x})+S_t(\mathbf{u})+S_t(\mathbf{0}_{n_1})$, and $y_j=\mathbf{0}_{m_1}$ for $j\neq t$. Fix t, and for each $\mathbf{u}$ in $\rho_t J_i(\mathcal{V})$ and $\mathbf{x}$ in $\mathbb{F}_2^{n_1}$, choose $(\mathbf{p}_\mathbf{u},\mathbf{q}_\mathbf{u},\mathbf{k}_\mathbf{u})$ from $\mathcal{V}$ such that $\rho_t J_i(\mathbf{p}_\mathbf{u},\mathbf{q}_\mathbf{u},\mathbf{k}_\mathbf{u})=\mathbf{u}$ and $(\mathbf{p}_\mathbf{x},\mathbf{q}_\mathbf{x},\mathbf{k}_\mathbf{x})$ from $\mathbb{F}_2^m\times\mathbb{F}_2^k$ such that $\rho_t J_i(\mathbf{p}_\mathbf{x},\mathbf{q}_\mathbf{x},\mathbf{k}_\mathbf{x})=\mathbf{x}$ and $\rho_j J_i(\mathbf{p}_\mathbf{x},\mathbf{q}_\mathbf{x},\mathbf{k}_\mathbf{x})=\mathbf{0}_{n_1}$ for all $j\neq t$. This is possible since we assumed that J_i is surjective. By (21), $U(F_i,\mathcal{V})$ contains the vector

$$\begin{aligned}&F_i(\mathbf{p}_x+\mathbf{p}_u,\ \mathbf{q}_x+\mathbf{q}_u,\ \mathbf{k}_x+\mathbf{k}_u)+F_i(\mathbf{p}_x,\mathbf{q}_x,\mathbf{k}_x)+F_i(\mathbf{p}_u,\mathbf{q}_u,\mathbf{k}_u)+F_i(\mathbf{0}_{\frac{1}{2}m},\mathbf{0}_{\frac{1}{2}m},\mathbf{0}_k)\\ &=[(\mathbf{0}_{\frac{1}{2}m},\mathbf{y}_1,\ldots,\mathbf{y}_l)],\end{aligned}$$

where

$$\begin{aligned}\mathbf{y}_j &= S_j(\rho_j J_i(\mathbf{p}_\mathbf{x},\mathbf{q}_\mathbf{x},\mathbf{k}_\mathbf{x})+\rho_j J_i(\mathbf{p}_\mathbf{u},\mathbf{q}_\mathbf{u},\mathbf{k}_\mathbf{u}))+\\ &\quad+S_j\rho_j J_i(\mathbf{p}_\mathbf{x},\mathbf{q}_\mathbf{x},\mathbf{k}_\mathbf{x})+S_j\rho_j J_i(\mathbf{p}_\mathbf{u},\mathbf{q}_\mathbf{u},\mathbf{k}_\mathbf{u})+S_j(\mathbf{0}_{n_1})\end{aligned}$$

for $j=1,\ldots,t$. But it is easy to check that $\mathbf{y}_t=S_j(\mathbf{x}+\mathbf{u})+S_j(\mathbf{x})+S_j(\mathbf{u})+S_j(\mathbf{0}_{n_1})$, while $\mathbf{y}_j=\mathbf{0}_{m_1}$ for $j\neq t$. This completes the proof of Lemma 4. □

In the lemma below we show that each DES-like cipher has a recursive linear structure comparable to the complementation property of DES. Let

$$\mathcal{C}_F = \left\{(\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0)\in\mathbb{F}_2^m\times\mathbb{F}_2^k:\ \begin{array}{l}L\mathbf{q}_0+K_i\mathbf{k}_0=\mathbf{0}_n \text{ for all odd } i \text{ in } \{1,\ldots,R\}\\ L\mathbf{p}_0+K_i\mathbf{k}_0=\mathbf{0}_n \text{ for all even } i \text{ in } \{1,\ldots,R\}\end{array}\right\}$$

(note that the equations contain $\mathbf{q}_0$ for odd i and $\mathbf{p}_0$ for even i). $\mathcal{C}_F$ is called the *complementation space* of F. Then we have:

LEMMA 5. *Let F be the DES-like cipher defined by* (18) *and* (19), *and let B be the identity on $\mathbb{F}_2^m$. Then $(\mathcal{C}_F,B)$ is a linear structure of F, which is recursive over $F_1,\ldots,F_R$.*

PROOF. Let $\mathcal{W}_i=[\mathbf{0}_m]$ for $0\leqslant i\leqslant R$ and

$\mathcal{V}_i=\mathcal{C}_F$ if $0\leqslant i\leqslant R$, i even;

$\mathcal{V}_i=\{(\mathbf{q}_0,\mathbf{p}_0,\mathbf{k}_0)\colon (\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0)\in\mathcal{C}_F\}$ if $0\leqslant i\leqslant R$, i odd.

From Lemma 2 we infer that for every subspace $\mathcal{V}=\bigoplus_{t=1}^{s}[(\mathbf{p}_t,\mathbf{q}_t,\mathbf{k}_t)]$ of $\mathbb{F}_2^m\times\mathbb{F}_2^k$

we have

$$T(F_i,\mathcal{V}) = \{\bigoplus_{t=1}^{s}[(\mathbf{q}_t,\mathbf{p}_t+S(L\mathbf{q}_t+K_i\mathbf{k}_t)+S(\mathbf{0}_{n_1})]\}\oplus U(F_i,\mathcal{V})\,. \qquad (23)$$

Using this fact together with Lemma 4 and the fact that $\mathcal{V}_{i-1}\subseteq ker(J_i)$ for $i=1,\ldots,R$, it follows that $\mathcal{V}_0,\ldots,\mathcal{V}_R$, $\mathcal{W}_0,\ldots,\mathcal{W}_R$ satisfy the relations (14) in Lemma 3. Since $\mathcal{V}_0=\mathcal{C}_F$ and $\mathcal{W}_R=[\mathbf{0}_m]$ this proves Lemma 5. □

Let F be defined by (18) and (19). To F we associate an *error propagation map* D_F, which maps every l-tuple $(\mathcal{X}_1,\ldots,\mathcal{X}_l)$ of subspaces of $\mathbb{F}_2^{m_1}$ to the l-tuple $(\mathcal{Y}_1,\ldots,\mathcal{Y}_l)$ of subspaces of $\mathbb{F}_2^{m_1}$ for which

$$\mathcal{Y}_j = U(S_j,\rho_j L(\mathcal{X}_1\times\cdots\times\mathcal{X}_l)) \text{ for } j=1,\ldots,l.$$

Any change in the plaintext or key affects in some way the outputs of the S-boxes after the first round. The effects on the outputs of the S-boxes propagate in the second round, and result in certain effects on the outputs of the S-boxes after the second round. Continuing in this way, the outputs of the S-boxes after each round are affected. Informally speaking, D_F describes, how the effects on the outputs of the S-boxes after some round propagate in the next round (the so-called *error propagation* in one round). Suppose that the spaces $\mathcal{X}_1,\ldots,\mathcal{X}_l$ describe the effects on the outputs of S-boxes $S_1,\ldots,S_l$, respectively, after the i-th round, say. Due to the linear mapping L, the effect on the output of S-box S_j causes some effect on the inputs of several S-boxes in the $(i+1)$-th round. The total effect on the input of S-box S_t, say, in round $i+1$, caused by the effects on the outputs of all S-boxes in round i, can be described by the space $\rho_t L(\mathcal{X}_1\times\cdots\times\mathcal{X}_l)$. Thus, the effect on the output of S_t after the $(i+1)$-th round is described by the space $\mathcal{Y}_t$. Intuitively speaking, if the spaces $\mathcal{Y}_t$ are larger, then the error propagation in one round is stronger. D_F^i (D_F iterated i times) describes the error propagation in i consecutive rounds. For F to be secure it is desirable that there is a number $P\leqslant R$ such that

$$D_F^P(\mathcal{X}_1,\ldots,\mathcal{X}_l) = (\mathbb{F}_2^{m_1},\ldots,\mathbb{F}_2^{m_1}) \qquad (24)$$

for all subspaces $\mathcal{X}_1,\ldots,\mathcal{X}_l$ of $\mathbb{F}_2^{m_1}$ with at least one $\neq[\mathbf{0}_{m_1}]$.

If P is the smallest integer for which (24) holds, then F is said to have *optimal error propagation after P rounds*. It seems that a good design criterion for a DES-like cipher is to make the number of rounds after which F has optimal error propagation as small as possible. For instance, this can be achieved by choosing S-boxes without non-trivial linear structures and choosing L in a careful way. It is easy to see that (24) holds if and only if $D_F^P(\mathcal{X}_1,\ldots,\mathcal{X}_l)=(\mathbb{F}_2^{m_1},\ldots,\mathbb{F}_2^{m_1})$ for every tuple of spaces $(\mathcal{X}_1,\ldots,\mathcal{X}_l)$, for which exactly one space is generated by a single non-zero vector, while the other spaces are $[\mathbf{0}_{m_1}]$. Hence in order to find the smallest P for which (24) holds, one merely has to compute $D_F^i(i=1,2,\ldots)$ for $l(2^{m_1}-1)$ tuples $(\mathcal{X}_1,\ldots,\mathcal{X}_l)$. This is feasible if l, m_1 and n_1 are small.

It also seems that another good design criterion for the DES-like cipher F

given by (18) and (19) is to choose the mappings L and $K_1,\ldots,K_R$ such that truncations of the DES-like cipher after a few rounds have no larger complementation space than the DES-like cipher itself. We say that F has *no extra complementation after Q rounds* if Q is the smallest integer for which the space

$$\left\{(\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0)\in\mathbb{F}_2^m\times\mathbb{F}_2^k:\ \begin{matrix} L\mathbf{p}_0+K_t\mathbf{k}_0=\mathbf{0}_n \text{ for all even } t\leqslant Q \\ L\mathbf{q}_0+K_t\mathbf{k}_0=\mathbf{0}_n \text{ for all odd } t\leqslant Q\end{matrix}\right\}$$

is equal to the complementation space $\mathcal{C}_F$. Provided that m, k and n are not too large, computing Q is feasible.

Below we give a sufficient condition for a DES-like cipher to have no non-trivial recursive linear structures other than that given in Lemma 5.

THEOREM 2. *Let F be the DES-like cipher given by* (18) *and* (19) *and suppose that the following three conditions are satisfied:*

(i) $U(S_j,\mathcal{U})\neq[\mathbf{0}_{m_1}]$ *for every subspace* $\mathcal{U}$ *of* $\mathbb{F}_2^{n_1}$ *with* $\mathcal{U}\neq[\mathbf{0}_{n_1}]$;

(ii) *F has optimal error propagation after P rounds and no extra complementation after Q rounds;*

(iii) $R>P+Q$.

Then for every linear structure $(\mathcal{V},B)$ that is recursive over $F_1,\ldots,F_R$ and for which $\mathcal{V}$ is not contained in $\mathcal{C}_F$, the mapping B is trivial.

PROOF. Let $\mathcal{V}_0,\ldots,\mathcal{V}_R$, $\mathcal{W}_0,\ldots,\mathcal{W}_R$ be a sequence of linear spaces satisfying the conditions of (14) (cf. Lemma 3) such that $\mathcal{V}_0$ is not contained in $\mathcal{C}_F$. We have to prove that $\mathcal{W}_R=\mathbb{F}_2^m$. To this end, we need two lemmas.

LEMMA 6. *Let $1\leqslant i\leqslant R-1$ and suppose that $\mathcal{W}_i\supseteq[\mathbf{0}_{m/2}]\times\mathcal{X}_1\times\cdots\times\mathcal{X}_l$, where $\mathcal{X}_1,\ldots,\mathcal{X}_l$ are subspaces of $\mathbb{F}_2^{m_1}$. Then $\mathcal{W}_{i+1}\supseteq[\mathbf{0}_{m/2}]\times\mathcal{Y}_1\times\cdots\times\mathcal{Y}_l$, where*

$$(\mathcal{Y}_1,\ldots,\mathcal{Y}_l)=D_F(\mathcal{X}_1,\ldots,\mathcal{X}_l).$$

PROOF. (14) implies that $\mathcal{W}_{i+1}\supseteq U(F_{i+1},\mathcal{W}_i\times[\mathbf{0}_k])$. Together with Lemma 4 this implies Lemma 6. □

LEMMA 7. *There is an i with $1\leqslant i\leqslant Q$ such that $\mathcal{W}_i\supseteq[\mathbf{0}_{m/2}]\times\mathcal{X}_1\times\cdots\times\mathcal{X}_l$, where $\mathcal{X}_1,\ldots,\mathcal{X}_l$ are subspaces of $\mathbb{F}_2^{m_1}$ of which at least one is $\neq[\mathbf{0}_{m_1}]$.*

PROOF. Let i be the smallest integer for which there is a $(\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0)\in\mathcal{V}_0$ such that either $L\mathbf{p}_0+K_i\mathbf{k}_0\neq\mathbf{0}_n$ and i even, or $L\mathbf{q}_0+K_i\mathbf{k}_0\neq\mathbf{0}_n$ and i odd. Then $1\leqslant i\leqslant Q$. By arguments similar to those in the proof of Lemma 5, one can show that

$$\begin{cases}\mathcal{V}_t\supseteq\mathcal{V}_0 \text{ for } 1\leqslant t<i \text{ and } t \text{ even},\\ \mathcal{V}_t\supseteq\{(\mathbf{q}_0,\mathbf{p}_0,\mathbf{k}_0):\ (\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0)\in\mathcal{V}_0\} \text{ for } 1\leqslant t<i \text{ and } t \text{ odd}.\end{cases}\tag{25}$$

Hence $J_i(\mathcal{V}_{i-1})\neq[\mathbf{0}_n]$. Put $\mathcal{X}_j=U(S_j,\rho_jJ_i(\mathcal{V}_{i-1}))$ for $j=1,\ldots,l$. By condition (i) of Theorem 2, at least one of the spaces $\mathcal{X}_j$ is $\neq[\mathbf{0}_{m_1}]$, and by (14) and

Lemma 4 we have $\mathcal{W}_i \supseteq U(F_i, \mathcal{V}_{i-1}) \supseteq [\mathbf{0}_{\frac{1}{2}m}] \times \mathcal{X}_1 \times \cdots \times \mathcal{X}_l$. This proves Lemma 7. □

We are now ready to complete the proof of Theorem 2. By Lemma 7 there is an i with $1 \leqslant i \leqslant Q$ and

$$\mathcal{W}_i \supseteq [\mathbf{0}_{\frac{1}{2}m}] \times \mathcal{X}_1 \times \cdots \times \mathcal{X}_l,$$

where $\mathcal{X}_1, \ldots, \mathcal{X}_l$ are subspaces of $\mathbb{F}_2^{m_1}$ of which at least one is $\neq [\mathbf{0}_{m_1}]$. By Lemma 6 we have for $t = 1, 2, \ldots$,

$$\mathcal{W}_{i+t} \supseteq [\mathbf{0}_{\frac{1}{2}m}] \times \mathcal{Y}_1 \times \cdots \times \mathcal{Y}_l \text{ with } (\mathcal{Y}_1, \ldots, \mathcal{Y}_l) = D_F^t(\mathcal{X}_1, \ldots, \mathcal{X}_l),$$

so that in particular,

$$\mathcal{W}_{i+P} \supseteq [\mathbf{0}_{\frac{1}{2}m}] \times \mathbb{F}_2^{\frac{1}{2}m}.$$

Since F has optimal error propagation after some number of rounds, there are subspaces $\mathcal{Z}_1, \ldots, \mathcal{Z}_l$ of $\mathbb{F}_2^{m_1}$ such that $D_F(\mathcal{Z}_1, \ldots, \mathcal{Z}_l) = (\mathbb{F}_2^{m_1}, \ldots, \mathbb{F}_2^{m_1})$. Hence $D_F(\mathbb{F}_2^{m_1}, \ldots, \mathbb{F}_2^{m_1}) = (\mathbb{F}_2^{m_1}, \ldots, \mathbb{F}_2^{m_1})$. Together with (14), Lemma 2 (or (23)) and Lemma 6 this implies that

$$\mathcal{W}_s = \mathbb{F}_2^m \text{ for } s > i + P.$$

But by condition (iii) we have $R > P + Q \geqslant i + P$. We conclude that $\mathcal{W}_R = \mathbb{F}_2^m$. □

We now prove Theorem 1. The same notation is used as in Section 5.

PROOF OF THEOREM 1. Let S, T be integers with $1 \leqslant S < T \leqslant 16$ and $T \geqslant S + 6$. It is easy to check that DES_{ST} is a DES-like cipher with parameters $m = 64$, $k = 56$, $n = 48$, $m_1 = 4$, $n_1 = 6$, $l = 8$, and $R = T - S + 1$. Further, $L = P_\lambda$ and $K_i = P_{\delta\kappa^{\omega(i+S-1)}}$ for $i = 1, \ldots, R$. The only data we need in the proof are the functions λ and κ, the integers $\omega(1), \ldots, \omega(16)$ and the linear structures in the S-boxes of DES, which are given in an appendix at the end of this paper. λ, κ and $\omega(1), \ldots, \omega(16)$ are such that for all S and T with $1 \leqslant S < T \leqslant 16$ and $T \geqslant S + 6$ and all $i \geqslant 4$, the space

$$\mathcal{C}_i = \left\{ (\mathbf{p}_0, \mathbf{q}_0, \mathbf{k}_0) \in \mathbb{F}_2^{64} \times \mathbb{F}_2^{56} : \begin{matrix} P_\lambda \mathbf{p}_0 + P_{\delta\kappa^{\omega(i+S-1)}} \mathbf{k}_0 = \mathbf{0}_{48} \text{ if } i \text{ even} \\ P_\lambda \mathbf{q}_0 + P_{\delta\kappa^{\omega(i+S-1)}} \mathbf{k}_0 = \mathbf{0}_{48} \text{ if } i \text{ odd} \end{matrix} \right\}$$

is equal to $[(\mathbf{1}_{64}, \mathbf{1}_{56})]$. Hence DES_{ST} has no extra complementation after Q rounds, for some integer $Q \leqslant 4$. By investigating λ and the linear structures in the S-boxes, it can be shown that each blockcipher DES_{ST} with $T \geqslant S + 6$ has optimal error propagation after $P := 2$ rounds. From the list of linear structures in the appendix it can be concluded that condition (i) of Theorem 2 also holds. Finally, $R \geqslant 7 > P + Q$. It can be verified in precisely the same way that DES_{ST}^{-1} is also a DES-like cipher satisfying the conditions of Theorem 2, provided that we interchange the two halves of its plaintext and ciphertext. Now Theorem 1 follows at once from Theorem 2. □

7. Possible extensions

Hellman et al. [10, IV] suggested the following way to break DES, which might also apply to an arbitrary DES-like cipher F: modify the S-boxes of F such that the resulting DES-like cipher F', with the modified S-boxes, is easy to break. If the modification in each S-box S is such that the output $S(\mathrm{x})$ is changed for only a few inputs x, then F and F' give the same ciphertexts for a non-negligible fraction of pairs of plaintexts and keys. For these plaintexts and keys, the key in F can be found by searching for the key in F'. Some of the potential possibilities of this attack were already discussed in [2, 2.1].

From the investigations in Section 6 it follows that recursive linear structures in DES-like ciphers are built up from linear structures in the S-boxes. Therefore, Hellman et al.'s attack described above might work if some of the S-boxes of a DES-like cipher have small *distances* to certain linear structures. Here the distance of an S-box to a particular linear structure $(\mathcal{V},B)$ is the minimal number of outputs of that S-box that must be changed to obtain an S-box with that linear structure $(\mathcal{V},B)$.

Ideally, one would choose the S-boxes such that they have large distances to all linear structures. A necessary (but probably not sufficient) condition for an S-box $S: \mathbb{F}_2^{n_1} \rightarrow \mathbb{F}_2^{m_1}$ to satisfy this, is that for each $\mathrm{x}_0 \in \mathbb{F}_2^{n_1}$ and for each linear mapping $B: \mathbb{F}_2^{m_1} \rightarrow \mathbb{F}_2$, the fraction of $\mathrm{x} \in \mathbb{F}_2^{n_1}$ for which $BS(\mathrm{x}+\mathrm{x}_0)=BS(\mathrm{x})$ is close to ½. For if $BS(\mathrm{x}+\mathrm{x}_0)=BS(\mathrm{x})$ for exactly f inputs x, then S has distance $\frac{1}{2}\min(f, 2^{n_1}-f)$ to the linear structure $([\mathrm{x}_0],B)$. It is not known if S-boxes exist with large distances to *all* linear structures, or if it is feasible to construct such S-boxes. However, not all linear structures in the S-boxes of a DES-like cipher will result in non-trivial linear structures of the whole cipher. Therefore, it suffices to find out which linear structures in the S-boxes are *dangerous*, in the sense that they would cause recursive linear structures in the DES-like cipher, and then choose S-boxes with large distances to only the dangerous linear structures.

It is known that S-box 4 of DES has non-trivial linear structures (cf. appendix). Further, structures like the so-called 50% and 25% exclusive-ors, found by Hellman. et al. (cf. [10, V]), and the correlation in each S-box between one of the six input bits and the modulo two sum of all four output bits, discovered independently by Shamir [16] and Franklin [9], show that each S-box of DES has small distances to certain linear structures. However, these structures have not been proved useful in the cryptanalysis of DES. It is yet unknown (from the open literature), whether the S-boxes in DES have distances to dangerous linear structures that are small enough to enable a known or chosen plaintext attack faster than exhaustive key search.

Acknowledgement

I would like to thank David Chaum for our many fruitful discussions on the subject of this paper and his suggestions to improve the presentation, and Evangelos Kranakis for his comments.

References

1. E.F. Brickell, J.H. Moore, M.R. Purtill (1987). Structure in the S-boxes of the DES. A.M. Odlyzko (ed.). *Proc. Crypto '86,* Lecture Notes in Computer Science 263, Springer-Verlag, New York, etc., 1-8.
2. D. Chaum, J.H. Evertse (1986). Cryptanalysis of DES with a reduced number of rounds; sequences of linear factors in blockciphers. H.C. Williams (ed.). *Proc. Crypto '85,* Lecture Notes in Computer Science 218, Springer-Verlag, Berlin etc., 192-211.
3. D.W. Davies, (1983). Some regular properties of the 'Data Encryption Standard' algorithm. D. Chaum, R.L. Rivest, A.T. Sherman (eds.). *Proc. Crypto '82,* Plenum, New York etc., 89-96.
4. M. Davio, Y. Desmedt, M. Fosseprez, R. Govaerts, J. Hulsbosch, P. Neutjens, P. Piret, J.J. Quisquater, J. Vandewalle, P. Wouters (1984). Analytical characteristics of the DES. D. Chaum (ed.). *Proc. Crypto '83,* Plenum, New York etc., 171-202.
5. Y. Desmedt, J.J. Quisquater, M. Davio (1985). Dependence of output on input in DES: Small avalanche characteristics. G.R. Blakley, D. Chaum (eds.). *Proc. Crypto '84,* Lecture Notes in Computer Science 196, Springer-Verlag, Berlin, etc., 359-376.
6. W. Diffie, M.E. Hellman (1967). A critique of the proposed data encryption standard. *Comm. ACM 19,* 164-165.
7. W. Diffie, M.E. Hellman (1977). Exhaustive cryptanalysis of the NBS Data Encryption Standard. *Computer 10,* 74-84.
8. J.H. Evertse. Linear structures in blockciphers. To appear in *Proc. Eurocrypt '87.*
9. M. Franklin (1985). M.Sc. Thesis, Univ. Berkeley.
10. M. Hellman, R. Merkle, R. Schroeppel, L. Washington, W. Diffie, S. Pohlig, P. Schweitzer (1976). *Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption Standard,* Information Systems Lab. Report SEL 76-042, Stanford University.
11. A.G. Konheim (1981). *Cryptography, a Primer,* J. Wiley & Sons, New York, etc.
12. C.H. Meyer (1978). Ciphertext/plaintext and ciphertext/key dependencies vs. number of rounds for the Data Encryption Standard. *AFIPS Conference Proceedings 47,* 1119-1126.
13. National Bureau of Standards (1977). Data Encryption Standard. *FIPS pub. 46,* U.S. Department of Commerce.
14. National Bureau of Standards (1980). DES modes of operation. *FIPS pub. 81,* U.S. Department of Commerce.
15. J.A. Reeds & J.L. Manferdelli (1984). DES has no per round linear factors. *Proc. Crypto '85,* 377-389.
16. A. Shamir (1985). On the security of DES. *Proc. Crypto '85,* 280-281.

Appendix

Linear structures in the S-boxes of DES

Below, we describe the spaces $U(S_j,\mathfrak{U})$ for each S-box S_j of DES and each subspace $\mathfrak{U}$ of $\mathbb{F}_2^6$.

$$U(S_j,\mathfrak{U}) = \mathbb{F}_2^4 \quad \text{for all } j \text{ in } \{1,...,8\}$$
$$\text{and all subspaces } \mathfrak{U} \text{ of } \mathbb{F}_2^6 \text{ with } \mathfrak{U} \neq [000000]$$

with the following exceptions:

$$\begin{aligned} U(S_4,[000001]) &= [1100]\oplus[0011] \\ U(S_4,[101110]) &= [1010]\oplus[0101] \\ U(S_4,[101111]) &= [1001]\oplus[0110] \\ U(S_4,[000001]\oplus[101110]) &= [1100]\oplus[1010]\oplus[0011] \end{aligned}$$

Description of λ

λ is given by a 12×4-table. The first row contains $\lambda(1),...,\lambda(12)$, the second row $\lambda(13),...,\lambda(24)$, etc.

25	16	7	20	21	29	21	29	12	28	17	1
17	1	15	23	26	5	26	5	18	31	10	2
10	2	8	24	14	32	14	32	27	3	9	19
9	19	13	30	6	22	6	22	11	4	25	16

Description of κ

κ is given as a product of two 28-cycles.

(	9	19	2	27	14	22	11	26	13	4	25	17	21	8
	5	24	7	16	6	10	20	18	28	12	3	15	23	1)
(	48	54	41	38	47	33	40	42	49	37	30	46	53	34
	44	51	35	31	52	39	45	56	50	32	55	43	36	29)

Table of $\omega(1), \ldots, \omega(16)$

$\omega(1), \ldots, \omega(16)$ are given from the left to the right.

1	2	4	6	8	12	14	15	17	19	21	23	25	27	28