LINEAR STRUCTURES IN BLOCKCIPHERS

Jan-Hendrik Evertse

Centre for Mathematics and Computer Science
Kruislaan 413 1098 SJ Amsterdam The Netherlands

§1. INTRODUCTION

A blockcipher maps each pair of plaintext and key onto a ciphertext in such a way that for every fixed key, the relationship between plaintexts and ciphertexts is one-to-one. It is assumed that plaintexts and ciphertexts belong to a message space comprising all bitstrings (sequences of zeros and ones) of a given length; keys are taken from a key space made up of all bitstrings of a possibly different given length. A well-known blockcipher is the NBS Data Encryption Standard (DES) [6], which is the iteration of sixteen essentially equal "rounds".

If a blockcipher is merely a linear mapping (with respect to exclusive-or) of the plaintext and key, then it is very easy to find an unknown key from a known pair of plaintext and corresponding ciphertext. Reeds and Manferdelli [7] pointed out that blockciphers with "partial linearity" are also vulnerable to a known plaintext attack much faster than exhaustive key search. We say that a blockcipher has partial linearity if there are non-injective linear mappings on the plaintext, key and ciphertext, respectively, and a "linear factor", which maps each pair of mapped plaintext and mapped key onto the mapped ciphertext. Given the plaintext and corresponding ciphertext, one can search for the unknown key by investigating the linear factor rather than the blockcipher itself. Reeds and Manferdelli considered the problem of whether DES has partial linearity. In [7], they proved that DES has no partial linearity caused by "per round linear factors", which means, roughly speaking, that DES has no partial linearity built up from the same kind of partial linearity in each round.

Chaum and Evertse [1] 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 linearity built up from possi-

This research was supported by the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

D. Chaum and W.L. Price (Eds.): Advances in Cryptology - EUROCRYPT '87, LNCS 304, pp. 249-266, 1988.

bly different kinds of partial linearity in the rounds. Chaum and Evertse also analysed blockciphers consisting of a reduced number of rounds of DES, and proved that blockciphers with less than five rounds of DES do have partial linearities caused by sequences of linear factors.

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. We discuss the cryptanalytic importance of linear structures and among other things, the linear structures of DES are investigated. It is shown that, as a consequence, blockciphers consisting of at least seven consecutive rounds of DES have no "recursive linear structures" other than the complementation property of DES; this means that apart from the complementation property, these blockciphers have no linear structures that can be built up from linear structures in the rounds. In fact, recursive linear structures are natural generalisations of sequences of linear factors. The results on DES just mentioned are derived from a general theorem on recursive linear structures in "DES-like ciphers" which we also prove.

In §2 we explain precisely what is meant by a linear structure in a blockcipher. More informally, one could say that a blockcipher has a linear structure if there are subsets P, K and C of plaintext bits, key bits and ciphertext bits of this blockcipher, respectively, such that for *each* plaintext and *each* key, a simultaneous change of all plaintext bits in P and all key bits in K has the *same* effect on the exclusive-or sum of the bits in C of the corresponding ciphertext; thus, either this exclusive-or sum is always changed or it always remains unchanged. Below we give a few examples of linear structures.

- The complementation property of DES (cf. [4]): simultaneously changing all bits of the plaintext and the key of DES results always in the change of all bits of the corresponding ciphertext.
- Bit independencies: the values of some ciphertext bits are independent of the values of certain plaintext bits and key bits; in other words, these ciphertext bits can be expressed as Boolean functions depending only on the other plaintext bits and key bits. It was pointed out in [5] and [1] that versions of DES with less than five rounds have such bit independencies.
- Structures that will change into linear structures when the blockcipher is modified by applying certain linear transformations (with respect to exclusive-or) to the plaintext, key and ciphertext respectively are linear structures themselves; for instance partial linearities are linear structures that change into bit independencies by applying appropriate linear transformations to the plaintext, ciphertext and key of the blockcipher.

We argue in §3 that 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 §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. As mentioned before, recursive linear structures in product ciphers are generalisations of the sequences of linear factors introduced in [1]. 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 is of any use in cryptanalysis.

In §5 we deal with DES-like ciphers. These are product ciphers built up in a similar way as DES from S-boxes, exclusive-or operations and mappings that are linear with respect to exclusive-or. 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 the S-boxes. Like DES, each DES-like cipher has a complementation property. The main result of §5 states, that any DES-like cipher satisfying certain easily verifiable conditions has apart from its complementation property no linear structures which are recursive over its rounds.

In §6 we show that each blockcipher consisting of seven or more consecutive rounds of DES is a DES-like cipher satisfying the conditions of the main result of §5. Therefore, blockciphers that consist of seven or more consecutive rounds of DES have no recursive linear structures other than the complementation property.

In §7 we explain briefly, that a DES-like cipher might be weak if some of its S-boxes have structures that change into linear structures by appropriately changing some of the output values of these S-boxes. Further, we discuss the relationship between the existence of such structures and the statistical properties of the S-boxes.

§2. NOTATION AND DEFINITIONS

In this section we introduce some notation to be used in the remainder of this paper, and give a formal definition of a linear structure in a blockcipher.

Let $\mathbb{F}_2=\{0,1\}$ be the finite field of two elements. When using notions from linear algebra such as vector spaces, linear mappings, etc., it is assumed that the underlying field of scalars is $\mathbb{F}_2$. 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 m bits in which the addition of two strings is just bitwise exclusive-or. Elements of $\mathbb{F}_2^m$ are denoted by $\mathbf{a}$, $\mathbf{b}$, etc.; $\mathbf{0}_m$ denotes the string of m zeros and $\mathbf{1}_m$ the string of m ones. Vectors in cartesian products $\mathbb{F}_2^{m_1}\times\cdots\times\mathbb{F}_2^{m_r}$ are often denoted as $(\mathbf{x}_1,\ldots,\mathbf{x}_r)$, where $\mathbf{x}_i\in\mathbb{F}_2^{m_i}$ for $i=1,\ldots,r$. $[\mathbf{x}]$ denotes the vector space generated by $\mathbf{x}$. If $\mathcal{V}_\alpha(\alpha\in A)$ are (linear) subspaces of the same vector space, then $\bigoplus_{\alpha\in A}\mathcal{V}_\alpha$ $=\{\sum_{\alpha\in A}x_\alpha\colon x_\alpha\in\mathcal{V}_\alpha\}$ denotes the smallest vector space containing each $\mathcal{V}_\alpha$. Thus,

$\bigoplus_{\alpha\in A}[\mathbf{x}_\alpha]$ denotes the vector space generated by the set of vectors $\{\mathbf{x}_\alpha\colon \alpha\in A\}$. For any linear mapping A with domain $\mathbb{F}_2^m$ we put $ker(A)=\{\mathbf{x}\in\mathbb{F}_2^m\colon A\mathbf{x}=\mathbf{0}\}$ and $im(A)=\{A\mathbf{x}\colon \mathbf{x}\in\mathbb{F}_2^m\}$. A linear mapping is said to be *trivial* if it maps every vector in its domain onto $\mathbf{0}$.

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

$$F_{\mathbf{k}}:=F(.,\mathbf{k})\colon \mathbb{F}_2^m\to\mathbb{F}_2^m \tag{1}$$

is invertible.

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 $(\mathcal{V},\mathcal{W})$, where $\mathcal{V}$ is a subspace of $\mathbb{F}_2^m\times\mathbb{F}_2^k$ and $\mathcal{W}$ a subspace of $\mathbb{F}_2^m$, such 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

$$F(\mathbf{p}+\mathbf{p}_0,\mathbf{k}+\mathbf{k}_0)+F(\mathbf{p},\mathbf{k})+F(\mathbf{p}_0,\mathbf{k}_0)+F(\mathbf{0}_m,\mathbf{0}_k)\in\mathcal{W}\,. \tag{2}$$

A linear structure $(\mathcal{V},\mathcal{W})$ is called *trivial* if $\mathcal{V}=[(\mathbf{0}_m,\mathbf{0}_k)]$ or $\mathcal{W}=\mathbb{F}_2^m$.

Remark 1. Each blockcipher has trivial linear structures.

Remark 2. It is easy to see that this definition implies that of §1. For let $(\mathcal{V},\mathcal{W})$ be a linear structure and let B be a linear mapping on $\mathbb{F}_2^m$ with $ker(B)=\mathcal{W}$. Then (2) implies that there is a function ψ, defined on $\mathcal{V}$, such that

$$\begin{aligned} BF(\mathbf{p}+\mathbf{p}_0,\mathbf{k}+\mathbf{k}_0)+BF(\mathbf{p},\mathbf{k}) \;=\; BF(\mathbf{p}_0,\mathbf{k}_0)+BF(\mathbf{0}_m,\mathbf{0}_k) \;=\; \psi(\mathbf{p}_0,\mathbf{k}_0)&\\ \text{for all } (\mathbf{p}_0,\mathbf{k}_0)\in\mathcal{V},\ \mathbf{p}\in\mathbb{F}_2^m \text{ and } \mathbf{k}\in\mathbb{F}_2^k.& \end{aligned} \tag{3}$$

In other words, if we fix $\mathbf{p}_0$ and $\mathbf{k}_0$, then exclusive-oring a plaintext with $\mathbf{p}_0$ and a key with $\mathbf{k}_0$ causes a change in the B-value of the corresponding ciphertext, which is for each plaintext and key the same.

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 $\mathrm{DES}(\mathbf{p}+\mathbf{1}_{64},\mathbf{k}+\mathbf{1}_{56})=\mathrm{DES}(\mathbf{p},\mathbf{k})+\mathbf{1}_{64}$ for every plaintext $\mathbf{p}$ and key $\mathbf{k}$. Hence $([(\mathbf{1}_{64},\mathbf{1}_{56})],\,[\mathbf{0}_{64}])$ is a linear structure of DES, and in (3) we can take for B the identity and 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 $\mathbf{k}$. Then $(\mathcal{V},\mathcal{W})$, with $\mathcal{V}=ker(A_1)\times ker(A_2)$ and $\mathcal{W}=ker(B)$, is the corresponding linear structure of F. The function ψ in (3) 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: $\mathbb{F}_2^m \times \mathbb{F}_2^k \rightarrow \mathbb{F}_2^m$ be a blockcipher and $(\mathcal{V},\mathcal{W})$ a linear structure of F. Further, let A,B be linear mappings with domains $\mathbb{F}_2^m \times \mathbb{F}_2^k$ and $\mathbb{F}_2^k$, respectively, such that $ker(A)=\mathcal{V}$ and $ker(B)=\mathcal{W}$. Then there exist a linear mapping C: $\mathbb{F}_2^m \times \mathbb{F}_2^k \rightarrow im(B)$ and a (not necessarily linear) mapping $\tilde{F}$: $im(A) \rightarrow im(B)$, 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 $(\mathcal{V},\mathcal{W})$ be a linear structure of F and A, B linear mappings with $ker(A)=\mathcal{V}$, $ker(B)=\mathcal{W}$. Further, let ψ be the function on $\mathcal{V}$, defined by (3) in §2. ψ is linear on $\mathcal{V}$ and therefore easy to compute from F, A and B. Indeed, let $(\mathbf{p}_0,\mathbf{k}_0)$, $(\mathbf{p}_1,\mathbf{k}_1)\in\mathcal{V}$. Then (3) implies that

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

Let A^* be a pseudo-inverse of A, that is a linear mapping A^*: $im(A)\rightarrow\mathbb{F}_2^m\times\mathbb{F}_2^k$ such that AA^* is the identity on $im(A)$. Such a pseudo-inverse exists and can be easily computed from A. Let D: $\mathbb{F}_2^m\times\mathbb{F}_2^k\rightarrow\mathbb{F}_2^m\times\mathbb{F}_2^k$ be the linear mapping defined by $D(\mathbf{p},\mathbf{k})=(\mathbf{p},\mathbf{k})+A^*A(\mathbf{p},\mathbf{k})$. Then $D(\mathbf{p},\mathbf{k})\in ker(A)=\mathcal{V}$ 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 (3) and the fact that $(\mathbf{p}_0,\mathbf{k}_0)\in\mathcal{V}$ imply that

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

This completes the proof of Lemma 1. □

In what follows, F: $\mathbb{F}_2^m\times\mathbb{F}_2^k\rightarrow\mathbb{F}_2^m$ is a blockcipher and $(\mathcal{V},\mathcal{W})$ a non-trivial linear structure of F, and A, B, C and $\tilde{F}$ are the mappings satisfying the conditions of Lemma 1. We define the linear mappings A_1, A_2, C_1 and C_2 by $A(\mathbf{p},\mathbf{k})=A_1\mathbf{p}+A_2\mathbf{k}$, $C(\mathbf{p},\mathbf{k})=C_1\mathbf{p}+C_2\mathbf{k}$. We describe two attacks: a known plaintext attack, where it is assumed that $0<n:=$dimension $ker(A_2)\leqslant k$; 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

$$\left.\begin{array}{l} A_2\mathbf{k}=\tilde{\mathbf{k}} \\ C_2\mathbf{k}=B\mathbf{c}+\tilde{F}(A_1\mathbf{p}+\tilde{\mathbf{k}})+C_1\mathbf{p} \end{array}\right\} \quad \text{in } \mathbf{k}\in\mathbb{F}_2^k \tag{4}$$

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 (4);

(ii) for each $\tilde{\mathbf{k}}$ in $im(A_2)$ for which (4) is soluble, he checks for each solution $\mathbf{k}$ of (4) if $F(\mathbf{p},\mathbf{k})=\mathbf{c}$.

Supposing that the 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. By a heuristic argument like in [1], §2, one can argue that the expected time in which the cryptanalist finds the key can be made smaller if he has more plaintext-ciphertext pairs for that same key.

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 [7] and [1] 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

$$A(\mathbf{p}_1,\mathbf{k}_1)=A(\mathbf{p}_2,\mathbf{k}_2)=\cdots=A(\mathbf{p}_N,\mathbf{k}_N). \tag{5}$$

Note that plaintexts $\mathbf{p}_1, \ldots, \mathbf{p}_N$ with this property exist if and only if $\mathcal{V}$ 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

$$C_2(\mathbf{k}'+\mathbf{k}_1+\mathbf{k}_i) = B\mathbf{c}_i+\tilde{F}A(\mathbf{p}_1,\mathbf{k}')+C_1\mathbf{p}_i \tag{6}$$

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 (5), (6) 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 as fast as that of exhaustive search.

Example 2: complementation property of DES. Hellman et al. ([4], §III) showed that there is a chosen plaintext attack on DES, using the complementation property, which is twice as fast as exhaustive key search. That attack is essentially the chosen plaintext attack just described, 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 such two pairs satisfy (5) 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 $F^*(\mathbf{p},\mathbf{k})=f(\mathbf{p}+\mathbf{k})+\mathbf{k}$. Then $(\mathcal{V},\mathcal{W})$ is a linear structure of F^*, with $\mathcal{V}=\{(\mathbf{x},\mathbf{x})\colon \mathbf{x}\in\mathbb{F}_2^m\}$ and $\mathcal{W}=[\mathbf{0}_m]$. Let $A:\mathbb{F}_2^m\times\mathbb{F}_2^m\to\mathbb{F}_2^m$ be the linear mapping given by $A(\mathbf{p},\mathbf{k})=\mathbf{p}+\mathbf{k}$; thus $ker(A)=\mathcal{V}$. Any N different plaintexts $\mathbf{p}_1,\ldots,\mathbf{p}_N$ of F^* satisfy condition (5) 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.

The chosen plaintext attack can also be used when $0<$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 into a chosen plaintext attack that is somewhat faster than the known plaintext attack described in this chapter. Further, it is possible to use linear structures in meet-in-the-middle attacks like in [1]. We do not work this out here.

§4. LINEAR STRUCTURES IN PRODUCT CIPHERS

Let $F_1,\ldots,F_R\colon \mathbb{F}_2^m\times\mathbb{F}_2^k\to\mathbb{F}_2^m$ be blockciphers. The *product* $F=F_R\cdots F_1$ of $F_1,\ldots,F_R$ is defined (cf. (1)) by

$$F_{\mathbf{k}}(\mathbf{p})=F_{R,\mathbf{k}}\cdots F_{1,\mathbf{k}}(\mathbf{p}) \tag{7}$$

(composition of mappings) 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. We describe how linear structures of F can be constructed from linear structures in $F_1,\ldots,F_R$. To this end, we introduce so-called T-spaces and U-spaces.

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

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

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

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 $U(F,\mathcal{V})\times[\mathbf{0}_k]\subseteq T(F,\mathcal{V})$. Obviously, (2) can be stated equivalently as

$$(\mathcal{V},\mathcal{W})\text{ linear structure of }F \Leftrightarrow U(F,\mathcal{V})\subseteq\mathcal{W}. \tag{8}$$

In other words, $U(F,\mathcal{V})$ is the minimal space $\mathcal{W}$ such that $(\mathcal{V},\mathcal{W})$ is a linear structure of F. The T-spaces are auxiliary spaces, needed to construct linear structures in blockciphers from linear structures in the rounds. For certain simple blockciphers like the rounds of DES the U-spaces are easy to compute. The next lemma describes how T-spaces can be computed from U-spaces.

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

$$T(F,\mathcal{V}) = \{U(F,\mathcal{V})\times[\mathbf{0}_k]\} \oplus \{\bigoplus_{i=1}^{s}[(F(\mathbf{p}_i,\mathbf{k}_i)+F(\mathbf{0}_m,\mathbf{0}_k),\mathbf{k}_i)]\}. \tag{9}$$

Proof. Denote the space at the right-hand side of (9) 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

$$(F(\mathbf{p}+\mathbf{p}_0,\mathbf{k}+\mathbf{k}_0)+F(\mathbf{p},\mathbf{k}),\mathbf{k}_0)\in\mathcal{X}. \tag{10}$$

Without loss of generality we may assume that $(\mathbf{p}_0,\mathbf{k}_0)=\sum_{i=1}^{t}(\mathbf{p}_i,\mathbf{k}_i)$, 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

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

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 linear structures of a single round of a blockcipher can be found by investigating the U-spaces of that round. The next lemma describes, how linear structures of the whole product cipher can be constructed from those T-spaces and U-spaces of the rounds satisfying some recurrence relation.

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

$$\left.\begin{array}{l} \mathcal{V}_i \supseteq T(F_i, \mathcal{V}_{i-1}), \\ \mathcal{W}_i \times [\mathbf{0}_k] \supseteq T(F_i, \mathcal{W}_{i-1} \times [\mathbf{0}_k]) \oplus \{U(F_i, \mathcal{V}_{i-1}) \times [\mathbf{0}_k]\} \text{ for } i = 1, \dots, R. \end{array}\right\} \tag{11}$$

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

(8) and Lemma 3 motivate the following:

Definition. Let $F_1, \dots, F_R$: $\mathbb{F}_2^m \times \mathbb{F}_2^k \rightarrow \mathbb{F}_2^m$ be blockciphers and put $F = F_R \cdots F_1$. A linear structure $(\mathcal{V}, \mathcal{W})$ of F is called *recursive* over $F_1, \dots, F_R$ if there are subspaces $\mathcal{V}_0, \dots, \mathcal{V}_R$ of $\mathbb{F}_2^m \times \mathbb{F}_2^k$ and $\mathcal{W}_0, \dots, \mathcal{W}_R$ of $\mathbb{F}_2^m$ for which (11) holds and for which $\mathcal{V} = \mathcal{V}_0$ and $\mathcal{W} = \mathcal{W}_R$.

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 can not exclude that a product cipher has linear structures that are *not* recursive over its rounds, and it might be a very difficult problem to check 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: $\mathbb{F}_2^m \times \mathbb{F}_2^k \rightarrow \mathbb{F}_2^m$ we have

$$T(HG, \mathcal{V}) \subseteq T(H, T(G, \mathcal{V})) \tag{12}$$

and

$$U(HG, \mathcal{V}) \times [\mathbf{0}_k] \subseteq T(H, U(G, \mathcal{V}) \times [\mathbf{0}_k]) \oplus \{U(H, T(G, \mathcal{V})) \times [\mathbf{0}_k]\}. \tag{13}$$

We first prove (12). 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

$$\begin{aligned} &(HG(\mathbf{p} + \mathbf{p}_0, \mathbf{k} + \mathbf{k}_0) + HG(\mathbf{p}, \mathbf{k}),\ \mathbf{k}_0) \\ &\qquad = (H(\mathbf{p}_1 + \tilde{\mathbf{p}}_0, \mathbf{k} + \mathbf{k}_0) + H(\mathbf{p}_1, \mathbf{k}),\ \mathbf{k}_0) \in T(H, T(G, \mathcal{V})). \end{aligned}$$

This proves (12).

We now prove (13). 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

$$\begin{aligned}\mathbf{a} &= H(\mathbf{p}_1+\mathbf{q}_2+\mathbf{q}_1,\mathbf{k}+\mathbf{k}_0)+H(\mathbf{p}_1+\mathbf{q}_2,\mathbf{k}+\mathbf{k}_0) \text{ and } (\mathbf{a},\mathbf{0}_k)\in T(H,\ U(G,\mathcal{V})\times[\mathbf{0}_k]),\\ \mathbf{b} &= H(\mathbf{p}_1+\mathbf{q}_2,\mathbf{k}+\mathbf{k}_0)+H(\mathbf{p}_1,\mathbf{k})+H(\mathbf{q}_2,\mathbf{k}_0)+H(\mathbf{0}_m,\mathbf{0}_k) \in U(H,\ T(G,\mathcal{V})),\\ \mathbf{c} &= H(\mathbf{p}_2+\mathbf{q}_2,\mathbf{k}_0+\mathbf{k}_0)+H(\mathbf{p}_2,\mathbf{k}_0)+H(\mathbf{q}_2,\mathbf{k}_0)+H(\mathbf{0}_m,\mathbf{0}_k) \in U(H,\ T(G,\mathcal{V})).\end{aligned}$$

This proves (13).

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

$$\mathcal{V}_i\supseteq T(F^{(i)},\mathcal{V}_0),\quad \mathcal{W}_i\supseteq U(F^{(i)},\mathcal{V}_0)\ \text{ for } i=1,\ldots,R, \tag{14}$$

which is obviously sufficient. (14) is trivially true for $i=1$. Suppose that (14) holds for $i=t-1$ (induction hypothesis). In the induction step, we apply (12) and (13) with $G=F^{(t-1)}$, $H=F_t$ and $\mathcal{V}=\mathcal{V}_0$. First we have, by (11), the induction hypothesis and (12), 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 (11), the induction hypothesis and (13), 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 (14) holds for $i=t$. This completes the induction step. □

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

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

This notion was introduced in [1]. 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 (11). Hence $(\mathcal{V}_0,\mathcal{W}_R)$ is a linear structure of F, which is recursive over $F_1,\ldots,F_R$.

† This definition is not consistent with that of a "linear factor" in [7] or in §1 of the present paper.

§5. 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, DES and Lucifer (after some slight modifications) and truncated versions of these product ciphers with a reduced number of rounds.

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

$$F=F_RF_{R-1}\cdots F_1, \tag{15}$$

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

$$F_i(\mathbf{p},\mathbf{q},\mathbf{k})=(\mathbf{q},\mathbf{p}+S(L\mathbf{q}+K_i\mathbf{k}))\text{ for }(\mathbf{p},\mathbf{q})\in\mathbb{F}_2^m,\ \mathbf{k}\in\mathbb{F}_2^k. \tag{16}$$

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

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

where $S_1,\ldots,S_l\colon\mathbb{F}_2^{n_1}\to\mathbb{F}_2^{m_1}$ are certain non-linear mappings (the S-boxes); $L\colon\mathbb{F}_2^{\frac{1}{2}m}\to\mathbb{F}_2^n$ is a linear mapping; and $K_1,\ldots,K_R\colon\mathbb{F}_2^k\to\mathbb{F}_2^n$ are linear mappings (the key scheduling) such that for $i=1,\ldots,R$, the linear mapping $J_i\colon\mathbb{F}_2^m\times\mathbb{F}_2^k\to\mathbb{F}_2^n$, given by

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

is surjective.

Linear structures in the rounds F_i can be described in terms of linear structures in the S-boxes, as defined below. 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 $\mathcal{U}$ of $\mathbb{F}_2^{n_1}$ we define the subspace

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

A linear structure of S_j is a pair $(\mathcal{U},\mathcal{X})$ for which $\mathcal{U}$ is a subspace of $\mathbb{F}_2^{n_1}$, $\mathcal{X}$ is a subspace of $\mathbb{F}_2^{m_1}$ and $U(S_j,\mathcal{U})\subseteq\mathcal{X}$; $(\mathcal{U},\mathcal{X})$ is said to be *trivial* if $\mathcal{U}=[\mathbf{0}_{n_1}]$ or $\mathcal{X}=\mathbb{F}_2^{m_1}$.

Let $\rho_j\colon\mathbb{F}_2^n\to\mathbb{F}_2^{n_1}$ 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 $\rho_jJ_i(\mathbf{p},\mathbf{q},\mathbf{k})$ 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* (16). *Further, let $\mathcal{V}$ be a subspace of $\mathbb{F}_2^m\times\mathbb{F}_2^k$. Then*

$$U(F_i,\mathcal{V}) = [\mathbf{0}_{\frac{1}{2}m}]\times\{U(S_1,\rho_1J_i(\mathcal{V}))\times U(S_2,\rho_2J_i(\mathcal{V}))\times\cdots\times U(S_l,\rho_lJ_i(\mathcal{V}))\}. \tag{17}$$

Proof. Denote the space on the right-hand side of (17) by $\mathfrak{Z}$. We first prove that $U(F_i,\mathcal{V})\subseteq\mathfrak{Z}$. 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 $(\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0)\in\mathcal{V}$ 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 $\mathbf{s}_j\in U(S_j,\rho_jJ_i(\mathcal{V}))$ 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

$$\begin{aligned}F_i(&\mathbf{p}+\mathbf{p}_0,\mathbf{q}+\mathbf{q}_0,\mathbf{k}+\mathbf{k}_0)+F_i(\mathbf{p},\mathbf{q},\mathbf{k})+F_i(\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0)+F_i(\mathbf{0}_{\frac{1}{2}m},\mathbf{0}_{\frac{1}{2}m},\mathbf{0}_k)\\ &= (\mathbf{0}_{\frac{1}{2}m},SJ_i(\mathbf{p}+\mathbf{p}_0,\mathbf{q}+\mathbf{q}_0,\mathbf{k}+\mathbf{k}_0)+SJ_i(\mathbf{p},\mathbf{q},\mathbf{k})+SJ_i(\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0)+SJ_i(\mathbf{0}_n))\\ &= (\mathbf{0}_{\frac{1}{2}m},\mathbf{s}_1,\ldots,\mathbf{s}_l),\end{aligned} \tag{18}$$

where

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

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

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

$$U(F_i,\mathcal{V})\supseteq[\mathbf{0}_{\frac{1}{2}m}]\times([\mathbf{0}_{m_1}]\times\cdots\times U(S_t,\rho_tJ_i(\mathcal{V}))\times\cdots\times[\mathbf{0}_{m_1}]), \tag{19}$$

where the space $U(S_t,\rho_tJ_i(\mathcal{V}))$ is preceded by $t-1$ spaces $[\mathbf{0}_{m_1}]$ and followed by $l-t$ spaces $[\mathbf{0}_{m_1}]$. In order to prove (19), it is sufficient to show that for each t in $\{1,\ldots,l\}$, $\mathbf{u}$ in $\rho_tJ_i(\mathcal{V})$ 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 $\rho_tJ_i(\mathcal{V})$ and $\mathbf{x}$ in $\mathbb{F}_2^{n_1}$, choose $(\mathbf{p_u},\mathbf{q_u},\mathbf{k_u})$ from $\mathcal{V}$ such that $\rho_tJ_i(\mathbf{p_u},\mathbf{q_u},\mathbf{k_u})=\mathbf{u}$ and $(\mathbf{p_x},\mathbf{q_x},\mathbf{k_x})$ from $\mathbb{F}_2^m\times\mathbb{F}_2^k$ such that $\rho_tJ_i(\mathbf{p_x},\mathbf{q_x},\mathbf{k_x})=\mathbf{x}$ and $\rho_jJ_i(\mathbf{p_x},\mathbf{q_x},\mathbf{k_x})=\mathbf{0}_{n_1}$ for all $j\neq t$. This is possible since we assumed that J_i is surjective. By (18), $U(F_i,\mathcal{V})$ 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

$$\begin{aligned}\mathbf{y}_j = S_j(&\rho_jJ_i(\mathbf{p_x},\mathbf{q_x},\mathbf{k_x})+\rho_jJ_i(\mathbf{p_u},\mathbf{q_u},\mathbf{k_u}))+\\ &+S_j\rho_jJ_i(\mathbf{p_x},\mathbf{q_x},\mathbf{k_x})+S_j\rho_jJ_i(\mathbf{p_u},\mathbf{q_u},\mathbf{k_u})+S_j(\mathbf{0}_{n_1})\end{aligned}$$

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

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

$\mathcal{C}_F$ is called the *complementation space* of F. Then we have:

Lemma 5. *Let F be the DES-like cipher defined by* (15) *and* (16). *Then* $(\mathcal{C}_F,[\mathbf{0}_m])$ *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

$$T(F_i,\mathcal{V}) = \left\{ \bigoplus_{t=1}^{s}[(\mathbf{q}_t,\mathbf{p}_t+S(L\mathbf{q}_t+K_i\mathbf{k}_t)+S(\mathbf{0}_{n_1}))] \right\} \oplus U(F_i,\mathcal{V}). \tag{20}$$

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 (11) 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 (15) and (16). 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 $i+1$-st 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 $i+1$-st round is described by the space $\mathcal{Y}_t$. Intuitively speaking, if the spaces $\mathcal{Y}_j$ 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

$$\begin{gathered} D_F^P(\mathcal{X}_1, \ldots, \mathcal{X}_l) = (\mathbb{F}_2^{m_1}, \ldots, \mathbb{F}_2^{m_1}) \\ \text{for all subspaces } \mathcal{X}_1, \ldots, \mathcal{X}_l \text{ of } \mathbb{F}_2^{m_1} \text{ with at least one } \neq [\mathbf{0}_{m_1}]. \end{gathered} \tag{21}$$

If P is the smallest integer for which (21) 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 (21) 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 (21) holds, one merely has to compute D_F^i $(i = 1, 2, \cdots)$ 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 (15) and (16) 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

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

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. *Let F be the DES-like cipher given by* (15) *and* (16) *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 $(\mathcal{V}, \mathcal{W})$ *that is recursive over* $F_1, \ldots, F_R$ *and for which* $\mathcal{V}$ *is not contained in* $\mathcal{C}_F$, *we have* $\mathcal{W} = \mathbb{F}_2^m$.

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 (11) (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 $\mathcal{W}_i \supseteq [\mathbf{0}_{\frac{1}{2}m}] \times \mathcal{X}_1 \times \cdots \times \mathcal{X}_l$, where $\mathcal{X}_1, \ldots, \mathcal{X}_l$ are subspaces of $\mathbb{F}_2^{m_1}$. Then $\mathcal{W}_{i+1} \supseteq [\mathbf{0}_{\frac{1}{2}m}] \times \mathcal{Y}_1 \times \cdots \times \mathcal{Y}_l$, where*

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

Proof. (11) 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 $\mathcal{W}_i \supseteq [\mathbf{0}_{\frac{1}{2}m}] \times \mathcal{X}_1 \times \cdots \times \mathcal{X}_l$, where $\mathcal{X}_1, \ldots, \mathcal{X}_l$ are subspaces of $\mathbb{F}_2^{m_1}$ of which at least one is $\neq [\mathbf{0}_{m_1}]$.*

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

$$\begin{cases} \mathcal{V}_t \supseteq \mathcal{V}_0 \text{ for } 1 \leqslant t < i \text{ and } t \text{ even,} \\ \mathcal{V}_t \supseteq \{(\mathbf{q}_0, \mathbf{p}_0, \mathbf{k}_0) \colon (\mathbf{p}_0, \mathbf{q}_0, \mathbf{k}_0) \in \mathcal{V}_0\} \text{ for } 1 \leqslant t < i \text{ and } t \text{ odd.} \end{cases} \tag{22}$$

Hence $J_i(\mathcal{V}_{i-1}) \neq [\mathbf{0}_n]$. Put $\mathcal{X}_j = U(S_j, \rho_j J_i(\mathcal{V}_{i-1}))$ for $j = 1, \ldots, l$. By condition (i) of the Theorem, at least one of the spaces $\mathcal{X}_j$ is $\neq [\mathbf{0}_{m_1}]$, and by (11) 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 the theorem. 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 $t = 1, 2, \cdots,$

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

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 (11), Lemma 2 (or (20)) 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 $\mathcal{W}_R = \mathbb{F}_2^m$. □

§6. APPLICATION TO DES

For convenience we modify DES a little bit: first, we do not use the tables IP and PC1 in the NBS-description (cf. [6]); and second, we combine the tables E and P, in the way described in [2], §3. Plaintexts and ciphertexts of DES are denoted by $(\mathbf{p},\mathbf{q})$, where $\mathbf{p},\mathbf{q} \in \mathbb{F}_2^{32}$.

DES is composed of the following mappings (cf. [6], [1]):
$P: \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$: bit permutation;
$E: \mathbb{F}_2^{32} \to \mathbb{F}_2^{48}$: bit expansion;
$S_l: \mathbb{F}_2^{6} \to \mathbb{F}_2^{4}$ $(l=1,\ldots,8)$: S-boxes;
$S: \mathbb{F}_2^{48} \to \mathbb{F}_2^{32}$: $S(\mathbf{x}_1,\ldots,\mathbf{x}_8)=(S_1\mathbf{x}_1,\ldots,S_8\mathbf{x}_8)$ for $\mathbf{x}_1,\ldots,\mathbf{x}_8 \in \mathbb{F}_2^6$;
$K_i: \mathbb{F}_2^{56} \to \mathbb{F}_2^{48}$ $(i=1,\ldots,16)$: key scheduling; all K_i are permuted choices of key bits, defined by PC2 and the shifting pattern.

Let F_i: $\mathbb{F}_2^{64} \times \mathbb{F}_2^{56} \to \mathbb{F}_2^{64}$ be the i-th round of DES, defined by

$$F_i(\mathbf{p},\mathbf{q},\mathbf{k})=(\mathbf{q},\mathbf{p}+S(EP\mathbf{q}+K_i\mathbf{k})) \text{ for } i=1,\ldots,16$$

and put

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

DES_{ST} is obviously a DES-like cipher with parameters $m=64$, $k=56$, $n=48$, $m_1=4$, $n_1=6$, $l=8$ and $R=T-S+1$. The complementation space of $DES_{1,16}$ is equal to $[(\mathbf{1}_{64},\mathbf{1}_{56})]$.

It follows from the Theorem of §5 that product ciphers, consisting of seven or more consecutive rounds of DES, have no non-trivial recursive linear structures other than the complementation property.

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

Proof. Put $R=T-S+1$, and let

$$\mathcal{C}_i = \left\{ (\mathbf{p}_0,\mathbf{q}_0,\mathbf{k}_0) \in \mathbb{F}_2^{64} \times \mathbb{F}_2^{56} \to \mathbb{F}_2^{64} : \begin{array}{l} EP\mathbf{p}_0+K_{i+S-1}\mathbf{k}_0=\mathbf{0}_{48} \text{ if } i \text{ even} \\ EP\mathbf{q}_0+K_{i+S-1}\mathbf{k}_0=\mathbf{0}_{48} \text{ if } i \text{ odd} \end{array} \right\}.$$

By examining EP and $K_1,\ldots,K_{16}$ (cf. [6]) it can be shown that for all S and T with $1 \leqslant S < T \leqslant 16$ and $T \geqslant S+6$ and all $i \geqslant 4$ we have $\mathcal{C}_i=[\mathbf{1}_{64},\mathbf{1}_{56}]$. Hence DES_{ST} has no extra complementation after Q rounds, for some integer $Q \leqslant 4$. By investigating the S-boxes and EP (see also [1], §§3,4) it can be shown that each blockcipher DES_{ST} with $T \geqslant S+6$ has optimal error propagation after $P:=2$ rounds. An investigation of the S-boxes implies that condition (i) of the Theorem holds. Finally, $R \geqslant 7 > P+Q$. Now the Corollary follows at once from the Theorem. □

Remark. The condition $T \geqslant S+6$ cannot be replaced by $T \geqslant S+5$. For instance, one can verify that $DES_{2,7}$ has a recursive linear structure $(\mathcal{V},\mathcal{W})$ for which $\mathcal{V}$ is not contained in $[(\mathbf{1}_{64},\mathbf{1}_{56})]$, whereas $\mathcal{W} \neq \mathbb{F}_2^{64}$.

§7. POSSIBLE EXTENSIONS

In [4], §IV, Hellman et al. 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 $S(\mathbf{x})$ is changed for only a few inputs $\mathbf{x}$, 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 [1], §2.1.

From the investigations in §5 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 is the minimal number of outputs of that S-box that must be changed to obtain an S-box with that linear structure.

There is a close relationship between the collection of distances of an S-box to all linear structures and the statistical properties of that S-box. Suppose that some S-box has an *A-linear structure*, that is a pair of subsets I, O of input bits and output bits, respectively, with the following property: for exactly a fraction A of those pairs of inputs of the S-box of which only the bits in I differ, the exclusive-or sum of the bits in O of the first corresponding output is equal to the exclusive-or sum of the bits in O of the second corresponding output. If $A=0$ or $A=1$ then that S-box has a linear structure. If $0<A<1$ then that S-box can be transformed to one with a linear structure by appropriately changing a fraction of $\frac{1}{2}\min(A, 1-A)$ of its outputs.

An S-box has maximal distance to each linear structure if each pair of subsets I, O of input bits and output bits, respectively, is a 50%-linear structure of that S-box. This is a strong requirement and it is not clear whether it is feasible to find S-boxes satisfying it. Not all linear structures in the S-boxes of some DES-like cipher will result in non-trivial recursive linear structures of that DES-like 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 the dangerous linear structures.

It is known that S-box 4 of DES has non-trivial linear structures (cf. [4], §V and [1], §4). Further, structures like the 50% and 25% exclusive-ors, found by Hellman et al. (cf. [4], §V), and the correlation in each S-box between one of the six input bits and the exclusive-or sum of all four output bits, discovered independently by Shamir [8] and

Franklin [3], 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 of this paper, and Evangelos Kranakis for his comments.

REFERENCES

[1] Chaum, D. & Evertse, J.-H, *Cryptanalysis of DES with a reduced number of rounds; sequences of linear factors in block ciphers,* in Advances in Cryptology: Proc. Crypto '85, H.C. Williams, ed., Lecture Notes in Computer Science 218, Springer Verlag, Berlin etc. (1986), pp. 192-211.

[2] Davio, M., Desmedt, Y., Fosseprez, M., Govaerts, R., Hulsbosch, J., Neutjens, P., Piret, P., Quisquater, J.J., Vandewalle, J., Wouters, P., *Analytical characteristics of the DES,* in Advances in Cryptology: Proc. Crypto '83, D. Chaum, ed., Plenum, New York (1984), pp. 171-202.

[3] Franklin, M., M.Sc. Thesis, Univ. Berkeley, May 1985.

[4] Hellman, M., Merkle, R., Schroeppel, R., Washington, L., Diffie, W., Pohlig, S., Schweitzer, P., *Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard,* Information Systems Lab. report SEL 76-042, Stanford University (1976).

[5] Meyer C.H. *Ciphertext / plaintext and ciphertext / key dependencies vs. number of rounds for the Data Encryption Standard,* AFIPS Conference Proceedings, 47, (June 1978), pp. 1119-1126.

[6] National Bureau of Standards, *Data Encryption Standard,* U.S. Department of Commerce, FIPS pub. 46 (January 1977).

[7] Reeds, J.A. & Manferdelli, J.L., *DES has no per round linear factors,* in Advances in Cryptology: Proc. Crypto '84, G.R. Blakley and D. Chaum, eds. Lecture Notes in Computer Science 196, Springer Verlag, Berlin etc. (1985), pp. 377-389.

[8] Shamir, A., *On the security of DES,* in Advances in Cryptology: Proc. Crypto '85, H.C. Williams, ed., Lecture Notes in Computer Science 218, Springer Verlag, Berlin etc. (1986), pp. 280-281.