CRYPTANALYSIS OF DES WITH A REDUCED NUMBER OF ROUNDS

SEQUENCES OF LINEAR FACTORS IN BLOCK CIPHERS

David Chaum & Jan-Hendrik Evertse

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

1. INTRODUCTION

A blockcipher is said to have a linear factor if, for all plaintexts and keys, there is a fixed non-empty set of key bits whose simultaneous complementation leaves the exclusive-or sum of a fixed non-empty set of ciphertext bits unchanged.

Since it appears infeasible to test all possible combinations of key bits and ciphertext bits for DES [NBS 77], we tried to find linear structures in the separate rounds of DES and hoped that these structures could be combined to yield a linear factor over the whole cipher. This naturally led us to the notion of "sequences of linear factors." In general, there might be linear factors that cannot be derived from sequences of linear factors, but under our assumptions about DES (detailed below) it seems that factors for the whole cipher would consist of sequences of factors for the individual rounds. Our notion of sequence of linear factors extends that of "per round linear factors" introduced by Reeds and Manferdelli [84]. The essential difference is that sequences of linear factors allow different rounds to have different linear factors, while per round linear factors must remain the same for each round.

We have given several examples of blockciphers, consisting of consecutive rounds of DES, that are vulnerable to a known plaintext attack faster than exhaustive key search. For instance, the blockciphers consisting of the first 4, 5 or 6 rounds of DES can be attacked about 2^{19}, 2^{9}, and 2^{2} faster than by exhaustive key search, respectively. The results presented do not work for the blockcipher consisting of rounds 1-7 of DES, but for the blockcipher consisting of rounds 2-8 we can save a factor 2.

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

The attacks considered are of the "meet-in-the-middle" type. Such an attack on a blockcipher composed of R consecutive rounds of DES can be described as follows: Suppose a cryptanalist has a plaintext **p** and corresponding ciphertext **c**. For each guessed key **k** the cryptanalist enciphers **p** with the first S rounds of DES yielding $\mathbf{d}'$, and deciphers **c** with the last $R-S$ rounds yielding $\mathbf{d}''$. If $\mathbf{d}'=\mathbf{d}''$, the cryptanalist concludes that **k** is the true key. Considerably less guesses for the key are required compared to exhaustive key search when there are i and j such that both the j-th bit of $\mathbf{d}'$ and the j-th bit of $\mathbf{d}''$ are independent of the i-th key bit. By independence we mean that for all **p**, **c**, and **k**, the j-th bit of $\mathbf{d}'$ and the j-th bit of $\mathbf{d}''$ are unchanged when the i-th bit of **k** is complemented.

Meyer [78] argued that blockciphers consisting of R consecutive rounds of DES can have ciphertext bits independent of key bits if and only if $R \leqslant 4$. In his arguments he used the unproved assumption that between two adjacent rounds of DES no dependencies are cancelled. This assumption means that if some output bit of the i-th round is functionally dependent on certain input bits for the i-th round and if some of these input bits are functionally dependent on the t-th key bit, then that output bit is also dependent on the t-th key bit. Meyer's assumption can be considered as a special case of the assumption that linear factors in DES always result from sequences of linear factors in the individual rounds. Under this general assumption, we show that blockciphers consisting of eight or more consecutive rounds of DES have no linear factors, and as a special case, that such ciphers are not subject to the kind of meet-in-the-middle attacks described above.

The next section explains how linear structures can be helpful in cryptanalysis while introducing some necessary notation. Subsequent sections consider whether DES with a reduced number of rounds has such structures. Potential extensions to more rounds of DES are mentioned in our concluding remarks.

2. LINEAR STRUCTURES IN BLOCKCIPHERS

This section gives an overview of various kinds of linear structures which blockciphers can have, together with their possible consequences for cryptanalysis. Some of the ideas in this section are included in [Hellman et al 76] and [Reeds and Manferdelli 84].

Some elementary notation that will allow us to make precise statements in the remainder of the paper is now introduced. Let $\mathbb{F}_2=\{0,1\}$ be the finite field of two elements. By $\mathbb{F}_2^n$ we shall denote the vector space of n-tuples over $\mathbb{F}_2$. Elements of $\mathbb{F}_2^n$ are denoted by bold characters such as **x** or strings $x_1x_2 \cdots x_n$, with $x_i \in \mathbb{F}_2$, and with the coordinates of **x** commonly referred to as "bits." Elements of the cartesian product $\mathbb{F}_2^{n_1} \times \cdots \times \mathbb{F}_2^{n_r}$ are often denoted by $(\mathbf{x}_1, \cdots, \mathbf{x}_r)$, where $\mathbf{x}_i \in \mathbb{F}_2^{n_i}$ for $i=1, \cdots, r$. When using notions from linear algebra, such as vectors, vector spaces, bases, linear mappings, etc. we assume that the underlying field of scalars is $\mathbb{F}_2$. In particular, the $+$ sign denotes addition of vectors over $\mathbb{F}_2$, sometimes referred to as exclusive-or. If A is a linear mapping, then $\mathrm{im}(A)$ and $\ker(A)$ will denote its image and null space, respectively. If $\mathcal{U}$ is a vector space and if $\mathcal{U}_1, \cdots, \mathcal{U}_r$ are subspaces of $\mathcal{U}$, then $\sum_{j=1}^{r} \mathcal{U}_j$ denotes the smallest subspace of $\mathcal{U}$ containing $\mathcal{U}_1, \cdots, \mathcal{U}_r$. The subspace of $\mathcal{U}$ generated by the set $\{\mathbf{x}_\alpha : \alpha \in A\}$ is denoted by $[\mathbf{x}_\alpha : \alpha \in A]$.

By a blockcipher, we mean a mapping $F : \mathcal{M} \times \mathcal{K} \to \mathcal{M}$, where $\mathcal{M} = \mathbb{F}_2^m, \mathcal{K} = \mathbb{F}_2^n$ are the message space and key space respectively, such that for each $\mathbf{k} \in \mathcal{K}$, the mapping $F(.,\mathbf{k}) : \mathcal{M} \to \mathcal{M}$ is invertible. We denote decryption by $F^{-1} : \mathcal{M} \times \mathcal{K} \to \mathcal{M}$, i.e. if $\mathbf{c} \in \mathcal{M}, \mathbf{k} \in \mathcal{K}$ then $F^{-1}(\mathbf{c},\mathbf{k})$ is equal to $\mathbf{p}$, where $\mathbf{p}$ is the element of $\mathcal{M}$ for which $F(\mathbf{p},\mathbf{k}) = \mathbf{c}$. Finally, if $F_1, \cdots, F_R : \mathcal{M} \times \mathcal{K} \to \mathcal{M}$ are blockciphers, then the product $F = F_R F_{R-1} \cdots F_1$ of $F_1, \cdots, F_R$ is defined as follows: if $\mathbf{p} \in \mathcal{M}, \mathbf{k} \in \mathcal{K}$, and if the sequence $\mathbf{p}_1, \mathbf{p}_2, \cdots$ is defined by

$$\mathbf{p}_1 = F_1(\mathbf{p},\mathbf{k}), \mathbf{p}_2 = F_2(\mathbf{p}_1,\mathbf{k}), \cdots, \mathbf{p}_r = F_r(\mathbf{p}_{r-1},\mathbf{k}),$$

then

$$F(\mathbf{p},\mathbf{k}) = \mathbf{p}_r.$$

Let $F : \mathcal{M} \times \mathcal{K} \to \mathcal{M}$ be a blockcipher, where $\mathcal{M} = \mathbb{F}_2^m$, $\mathcal{K} = \mathbb{F}_2^n$. If $\mathbf{c} = F(\mathbf{p},\mathbf{k})$ with $\mathbf{p} = p_1 \cdots p_m$, $\mathbf{k} = k_1 \cdots k_n, \mathbf{c} = c_1 \cdots c_m$, then

$$c_i = f_i(p_1, \cdots, p_m, k_1, \cdots, k_n) \quad \text{for} \quad i = 1, \cdots, m, \tag{1}$$

where the $f_i : \mathbb{F}_2^{m+n} \to \mathbb{F}_2$ are boolean functions. Suppose that there are sets $\{i_1, \cdots, i_s\} \subseteq \{1, \cdots, n\}, \{j_1, \cdots, j_r\} \subseteq \{1, \cdots, m\}$ such that the functions f_{j_k} are independent of the key bits k_i with i different from $i_1, \cdots, i_s$, that is

$$c_{j_k} = f_{j_k}(p_1, \cdots, p_m, k_{i_1}, \cdots, k_{i_s}) \quad \text{for} \quad k = 1, \ldots, r.$$

This can be written more conveniently as

$$\tilde{\mathbf{c}} = \tilde{F}(\mathbf{p}, \tilde{\mathbf{k}}), \tag{2}$$

where $\tilde{\mathbf{k}} = k_{i_1} \cdots k_{i_s}$, $\tilde{\mathbf{c}} = c_{j_1} \cdots c_{j_r}$, $\tilde{F} : \mathbb{F}_2^m \times \mathbb{F}_2^s \to \mathbb{F}_2^r$.

Suppose that a cryptanalist knows a pair of plaintext and corresponding ciphertext $(\mathbf{p},\mathbf{c})$ of F and wants to find the key $\mathbf{k}$ from the equation

$$\mathbf{c} = F(\mathbf{p},\mathbf{k}). \tag{3}$$

The cryptanalist may use the following method: (i) solve $\tilde{\mathbf{k}} = k_{i_1} \cdots k_{i_s}$ from (2) by exhaustively trying all $\tilde{\mathbf{k}}$ (a value of $\tilde{\mathbf{k}}$ can be tried by extending $\tilde{\mathbf{k}}$ to a key $\mathbf{k}$ by setting all key bits k_i with i different from $i_1, \cdots, i_s$ to zero, computing $F(\mathbf{p},\mathbf{k})$ and checking if the correct value of $\tilde{\mathbf{c}}$ appears) and (ii) solve $\mathbf{k}$ from (3) by exhaustively trying all $\mathbf{k}$ for which $k_{i_1}, \cdots, k_{i_s}$ are equal to the values found in (i). Assuming that in step (i) only one solution is found, the cryptanalist has to do about

$$2^s+2^{n-s} \tag{4}$$

computations of F before finding the key. In general, we may not assume that only one solution is found in (i). The number of solutions found in (i) can be reduced if the cryptanalist possesses M pairs of corresponding plaintext and ciphertext. Suppose that the cryptanalist has the plaintext-ciphertext pairs $(\mathbf{p}_1,\mathbf{c}_1), \cdots ,(\mathbf{p}_M,\mathbf{c}_M)$ and wants to solve the key from

$$\mathbf{c}_1=F(\mathbf{p}_1,\mathbf{k})\ , \cdots ,\ \mathbf{c}_M=F(\mathbf{p}_M,\mathbf{k}). \tag{5}$$

Instead of doing (i),(ii), the following method may be used:

(i'): try all values for $\tilde{\mathbf{k}}$. If a $\tilde{\mathbf{k}}$ is found with $\tilde{F}(\mathbf{p}_1,\tilde{\mathbf{k}})=\tilde{\mathbf{c}}_1$, then check if $\tilde{F}(\mathbf{p}_2,\tilde{\mathbf{k}})=\tilde{\mathbf{c}}_2$, $\tilde{F}(\mathbf{p}_3,\tilde{\mathbf{k}})=\tilde{\mathbf{c}}_3, \cdots$ until some i is found with $\tilde{F}(\mathbf{p}_i,\tilde{\mathbf{k}})\neq\tilde{\mathbf{c}}_i$ or $i=M$. Accept $\tilde{\mathbf{k}}$ as a solution if $\tilde{F}(\mathbf{p}_i,\tilde{\mathbf{k}})= \tilde{\mathbf{c}}_i$ for $i=1, \cdots ,M$;

(ii'): try all values for $\mathbf{k}$ for which $k_{i_1} \cdots k_{i_s}$ is equal to one of the accepted solutions in (i'). If $F(\mathbf{p}_1,\mathbf{k})=\mathbf{c}_1$ then check if $F(\mathbf{p}_2,\mathbf{k})=\mathbf{c}_2$, $F(\mathbf{p}_3,\mathbf{k})=\mathbf{c}_3, \cdots$ until $F(\mathbf{p}_i,\mathbf{k})\neq\mathbf{c}_i$ for some i or $i=M$. Accept $\mathbf{k}$ as a correct key if $F(\mathbf{p}_i,\mathbf{k})=\mathbf{c}_i$ for $i=1, \cdots ,M$.

This algorithm finds all keys $\mathbf{k}$ with $F(\mathbf{p}_i,\mathbf{k})=\mathbf{c}_i$ for $i=1, \cdots ,M$. In order to estimate the expected number of encipherments needed in steps (i'),(ii') we make the following very heuristic assumptions: for $k=1, \cdots ,r$, $i=1, \cdots ,M$ and for all wrong values of $\tilde{\mathbf{k}}=k_{i_1} \cdots k_{i_s}$ the $f_{j_k}(\mathbf{p}_i,\tilde{\mathbf{k}})$ are mutually independent uniformly distributed random variables on $\{0,1\}$; for all j different from $j_1, \cdots ,j_r$, for all i in $\{1, \cdots ,M\}$ and all wrong values of $\mathbf{k}$ the $f_j(\mathbf{p}_i,\mathbf{k})$ are also mutually independent uniformly distributed random variables on $\{0,1\}$. With these assumptions, the expected number of encipherments in step (i') is

$$\begin{aligned} &M+(2^s-1)(1-2^{-r})\times(1+2\times2^{-r}+3\times2^{-2r}+ \cdots) \\ &\leqslant M+\frac{2^s}{1-2^{-r}} \end{aligned}$$

(where the term M comes from the correct value of $\tilde{\mathbf{k}}$). The expected number of keys which have to be tried in step (ii') is equal to the product of $2^{n-s}$and the expected number of accepted values for $\tilde{\mathbf{k}}$ in step (i'), namely

$$2^{n-s}\left[1+(2^s-1)2^{-Mr}\right].$$

Hence the expected number of encipherments in step (ii') is at most

$$M+\left[2^{n-s}\left[1+(2^s-1)2^{-Mr}\right]-1\right](1-2^{r-m})\times$$
$$\times\left[1+2\times 2^{r-m}+3\times 2^{2(r-m)}+\cdots\right]$$

$$\leqslant M+\frac{2^{n-s}+2^{n-Mr}}{1-2^{r-m}}.$$

Therefore, the expected total number of encipherments is at most

$$2M+\frac{2^s}{1-2^{-r}}+\frac{2^{n-s}+2^{n-Mr}}{1-2^{r-m}}. \tag{6}$$

If $Mr>s$ this is only slightly larger than 2^s+2^{n-s}.

Suppose that $G,H:\mathcal{M}\times\mathcal{K}\to\mathcal{M}$ are two blockciphers and that $F=HG$. Suppose that a cryptanalist knows a plaintext-ciphertext pair of F, $(\mathbf{p},\mathbf{c})$ say. Instead of solving the unknown key $\mathbf{k}$ from (3), a cryptanalist can try to solve $\mathbf{k}$ from

$$G(\mathbf{p},\mathbf{k})=H^{-1}(\mathbf{c},\mathbf{k}). \tag{7}$$

Attacks in which $\mathbf{k}$ is solved from eq. (7) instead of (3) are called *meet-in-the-middle attacks.* Let $\mathbf{d}'=d'_1\cdots d'_m=G(\mathbf{p},\mathbf{k})$, $\mathbf{d}''=d''_1\cdots d''_m=H^{-1}(\mathbf{c},\mathbf{k})$. Suppose that there are subsets $\{i_1,\cdots,i_s\}$ of $\{1,\dots,n\}$ and $\{j_1,\cdots,j_r\}$ of $\{1,\dots,m\}$ such that $d'_{j_1},\cdots,d'_{j_r}$, $d''_{j_1},\cdots,d''_{j_r}$ are functionally independent of the key bits k_i with i different from $i_1,\cdots,i_s$. In other words, there are boolean functions $g_1,\cdots,g_r$, $h_1,\cdots,h_r$ such that

$$\begin{array}{ll} d'_{j_1}=g_1(\mathbf{p},k_{i_1},\cdots,k_{i_s}) & d''_{j_1}=h_1(\mathbf{c},k_{i_1},\cdots,k_{i_s}) \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ d'_{j_r}=g_r(\mathbf{p},k_{i_1},\cdots,k_{i_s}) & d''_{j_r}=h_r(\mathbf{c},k_{i_1},\cdots,k_{i_s}) \end{array} \tag{8}$$

Now the unknown key $\mathbf{k}$ can be found by first solving $k_{i_1},\cdots,k_{i_s}$ from $g_1=h_1,\cdots,g_r=h_r$ and then solving the remaining key bits from (3) or (7). If the cryptanalist has M plaintext-ciphertext pairs, the number of G,H^{-1} computations needed is given by (6).

We now consider linear structures more general than independencies of ciphertext bits or "bits in the middle" from key bits. Suppose that $A:\mathbb{F}_2^m\to\mathbb{F}_2^r, B:\mathbb{F}_2^n\to\mathbb{F}_2^s$ are surjective linear mappings and that there exists a function $\tilde{F}$ such that

$$AF(\mathbf{p},\mathbf{k})=\tilde{F}(\mathbf{p},B\mathbf{k}) \text{ for } \mathbf{p}\in\mathcal{M},\ \mathbf{k}\in\mathcal{K}. \tag{9}$$

Given a known plaintext-ciphertext pair $(\mathbf{p},\mathbf{c})$ it is possible to solve the unknown key $\mathbf{k}$ from $\mathbf{c}=F(\mathbf{p},\mathbf{k})$ by firstly solving $\tilde{\mathbf{k}}$ from $A\mathbf{c}=\tilde{F}(\mathbf{p},\tilde{\mathbf{k}})$ and secondly solving $\mathbf{k}$ from $\mathbf{c}=F(\mathbf{p},\mathbf{k})$, under the restriction that $A\mathbf{k}=\tilde{\mathbf{k}}$. Using that $\mathrm{im}(A)$ has cardinality 2^s while the equation $A\mathbf{k}=\tilde{\mathbf{k}}$ has 2^{n-s} solutions, a cryptanalist having M plaintext-ciphertext pairs can find the key in a number of encipherments which is given by (6).

The linear structures which can be used in a meet-in-the-middle attack are more general than those explained above. Such structures exist if there are blockciphers G,H with $F=HG$, surjective linear mappings $A:\mathbb{F}_2^m\rightarrow\mathbb{F}_2^r, B:\mathbb{F}_2^n\rightarrow\mathbb{F}_2^s$ and functions $\tilde{G},\tilde{H}$, such that for $\mathbf{p},\mathbf{c}\in\mathcal{M},\mathbf{k}\in\mathcal{K}$,

$$AG(\mathbf{p},\mathbf{k})=\tilde{G}(\mathbf{p},B\mathbf{k}), \quad AH^{-1}(\mathbf{c},\mathbf{k})=\tilde{H}(\mathbf{c},B\mathbf{k}). \tag{10}$$

As mentioned in the introduction, given a blockcipher F, it might be infeasible to find out if it has any linear factors. Instead of this, one might try to represent F as a product of cryptographically weak blockciphers and check if these weak blockciphers themselves have such linear structures. Suppose that $F_1, \cdots, F_R$: $\mathcal{M}\times\mathcal{K}\rightarrow\mathcal{M}$ are blockciphers and that $F=F_R \cdots F_1$. Let A_i $(i=0, \cdots, R)$ be linear mappings on $\mathcal{M}$ and let B be a linear mapping on $\mathcal{K}$. We call $(A_0, \cdots, A_R;B)$ a *sequence of linear factors* for F (with respect to $F_1, \cdots, F_R$) if there are functions $\tilde{F}_i$ $(i=0, \cdots, R)$: $\mathrm{im}(A_{i-1})\times\mathrm{im}(B)\rightarrow\mathrm{im}(A_i)$ such that for $\mathbf{p}\in\mathcal{M},\mathbf{k}\in\mathcal{K}$,

$$A_iF_i(\mathbf{p},\mathbf{k})=\tilde{F}_i(A_{i-1}\mathbf{p},B\mathbf{k}) \quad \text{for } i=1, \cdots, R. \tag{11}$$

Then there is a function $\tilde{F}:\mathrm{im}(A_0)\times\mathrm{im}(B)\rightarrow\mathrm{im}(A_R)$ such that

$$A_RF(\mathbf{p},\mathbf{k}) \;=\; \tilde{F}(A_0\mathbf{p},B\mathbf{k}). \tag{12}$$

Note again that there may be linear mappings A_0,A_R,B satisfying (12) for some $\tilde{F}$ which do not belong to sequences of linear factors.

Let $G=F_MF_{M-1} \cdots F_1$, $H=F_RF_{R-1} \cdots F_{M+1}$. Then $F=HG$. In a meet-in-the-middle attack we will need sequences of linear factors $(A_0, \cdots, A_M;B),(A'_R,A'_{R-1}, \cdots, A'_M;B)$ for G,H^{-1} respectively, such that

$$A_M=A'_M.$$

Also note that if $(A'_R, \cdots, A'_M;B)$ is a sequence of linear factors for H^{-1} then $(A'_M, \cdots, A'_R;B)$ is not necessarily a sequence of linear factors for H.

We need no longer distinguish between sequences of linear factors $(A_0, \cdots, A_R;B)$, $(A'_0, \cdots, A'_R;B')$ with $\ker(A_i)=\ker(A'_i)$ $(i=0, \cdots, R)$, $\ker(B)=\ker(B')$, since they give us exactly the same advantage in finding the key. Thus we are mainly interested in sequences of vector spaces $(\mathcal{V}_0,\mathcal{V}_1, \cdots, \mathcal{V}_R;\mathcal{W})$ where $\mathcal{V}_i=\ker(A_i),\mathcal{W}=\ker(B)$ for some sequence of linear factors $(A_0, \cdots, A_R;B)$. Such sequences of vector spaces are called *sequences of factor spaces* for F. The following lemma characterizes these sequences of factor spaces.

Lemma 1 . *Let $\mathcal{V}_0, \cdots ,\mathcal{V}_R \subseteq \mathcal{M}$, $\mathcal{W} \subseteq \mathcal{K}$ be vector spaces. Then the following statements are equivalent.*

(i) $(\mathcal{V}_0, \cdots ,\mathcal{V}_R;\mathcal{W})$ is a sequences of factor spaces for F.

(ii) $F_i(\mathbf{p}+\mathbf{x},\mathbf{k}+\mathbf{y})+F_i(\mathbf{p},\mathbf{k}) \in \mathcal{V}_i$
for all $i \in \{1, \cdots ,R\}$,$\mathbf{p} \in \mathcal{M}$,$\mathbf{k} \in \mathcal{K}$,$\mathbf{x} \in \mathcal{V}_{i-1}$,$\mathbf{y} \in \mathcal{W}$.

Proof: (i)→(ii). Let $(A_0, \cdots ,A_R;B)$ be a sequence of linear factors for F with $\ker(A_i)=\mathcal{V}_i$ $(i=0, \cdots ,R)$, $\ker(B)=\mathcal{W}$. It is easy to check, that for $i=1, \cdots ,R,\mathbf{p} \in \mathcal{M},\mathbf{k} \in \mathcal{K}$, $\mathbf{x} \in \mathcal{V}_{i-1}$, $\mathbf{y} \in \mathcal{W}$,

$$A_iF_i(\mathbf{p}+\mathbf{x},\mathbf{k}+\mathbf{y})=A_iF_i(\mathbf{p},\mathbf{k}).$$

This proves (ii).

(ii)→(i). Choose linear mappings $A_0, \cdots A_R,B$ such that $\ker(A_i)=\mathcal{V}_i$ $(i=0, \cdots ,R)$, $\ker(B)=\mathcal{W}$. Define functions $\tilde{F}_i$: $\mathrm{im}(A_{i-1}) \times \mathrm{im}(B) \rightarrow \mathrm{im}(A_i)$ $(i=1, \cdots ,R)$ as follows: if $\tilde{\mathbf{p}} \in \mathrm{im}(A_{i-1}),\tilde{\mathbf{k}} \in \mathrm{im}(B)$ then choose $\mathbf{p},\mathbf{k}$ such that $A_{i-1}\mathbf{p}=\tilde{\mathbf{p}},B\mathbf{k}=\tilde{\mathbf{k}}$ and put $\tilde{F}_i(\tilde{\mathbf{p}},\tilde{\mathbf{k}})= A_iF_i(\mathbf{p},\mathbf{k})$. From statement (ii) it follows that the $\tilde{F}_i$ are well-defined (i.e. independent of the choice of $\mathbf{p},\mathbf{k}$) and that for $\mathbf{p} \in \mathcal{M},\mathbf{k} \in \mathcal{K}$,

$$A_iF_i(\mathbf{p},\mathbf{k}) = \tilde{F}_i(A_{i-1}\mathbf{p},B\mathbf{k}).$$

This proves (i). □

2.1. SOME GENERALIZATIONS

Here we briefly mention some ways in which sequences of linear factors can be generalized. We have not looked for such general structures in DES. As before, $F_1, \cdots ,F_R$ are blockciphers and $F=F_RF_{R-1} \cdots F_1$. One possibility is to consider sequences of factors $(A_0, \cdots ,A_R;B)$ where $A_0, \cdots ,A_R;B$ are not necessarily linear mappings satisfying (11) for certain functions $\tilde{F}_i$. Such sequences can be helpful in cryptanalysis if B is a simple mapping, such as a linear mapping, a mapping composed of low degree polynomials over $\mathbb{F}_2$, etc.

A second generalization considers sequences of *near* linear factors. This notion is an extension of an idea presented in [Hellman et al 76]. A sequence of linear mappings $(A_0, \cdots ,A_R;B)$ is called a sequence of near linear factors for F valid for a set $\mathcal{S}$ of pairs of plaintexts and keys if there are functions $\tilde{F}_i$ such that for each pair $(\mathbf{p},\mathbf{k})$ in $\mathcal{S}$ and each i with $1 \leqslant i \leqslant R$,

$$A_i\mathbf{p}_i=\tilde{F}_i(A_{i-1}\mathbf{p}_{i-1},B\mathbf{k}) ,$$

where $\mathbf{p}_0=\mathbf{p}$, $\mathbf{p}_i=F_i(\mathbf{p}_{i-1},\mathbf{k})$. Suppose that F has a sequence of near linear factors $(A_0, \cdots ,A_R;B)$ valid for a set $\mathcal{S}$ containing pairs $(\mathbf{p},\mathbf{k})$ for each key $\mathbf{k}$ or more generally, that F has sequences of linear factors $(A_0, \cdots ,A_R;B)$, all having the same A_0,A_R,B and valid for sets

$\mathbb{S}_1, \cdots, \mathbb{S}_r$ respectively, such that $\mathbb{S}_1 \cup \cdots \cup \mathbb{S}_r$ contains pairs $(\mathbf{p},\mathbf{k})$ for each $\mathbf{k}$. Then there exist a positive number C and a function $\tilde{F}$ such that for each key $\mathbf{k}$, the relations

$$A_R F(\mathbf{p},\mathbf{k}) = \tilde{F}(A_0\mathbf{p}, B\mathbf{k}) \tag{13}$$

are valid for a fraction $\frac{1}{C}$ of the plaintexts $\mathbf{p}$. If a cryptanalist has C pairs of corresponding plaintext and ciphertext, then for each pair $(\mathbf{p},\mathbf{c})$ the key can be solved, under the hypothesis that (13) holds for the plaintext $\mathbf{p}$. Thus C keys are found, one of which is expected to be the correct key.

A blockcipher F is said to have key clustering if there exist a mapping $\tilde{F}$ and a non-injective linear mapping B such that for each key $\mathbf{k}$, the relation

$$F(\mathbf{p},\mathbf{k}) = \tilde{F}(\mathbf{p}, B\mathbf{k})$$

holds for a positive fraction of the plaintexts $\mathbf{p}$. Desmedt, Quisquater and Davio [84] gave a few examples of key clustering in blockciphers consisting of at most three rounds of DES. The method by which these examples have been constructed can be described in terms of sequences of near linear factors as mentioned above.

3. MEET-IN-THE-MIDDLE ATTACKS ON DES

Independencies of "bits in the middle" from key bits in DES, which can be helpful in a meet-in-the-middle attack, are the subject of this section. First we give an overview of the mappings used in DES, assuming that the reader is familiar with the NBS description of the Data Encryption Standard. (For the complete description, we refer to [NBS 77]). In this paper, we use a slightly modified version of DES in which $IP, IP^{-1}, PC1$ are not used and E,P are combined to one table EP (cf. Davio et al [83], pp. 184-185). Thus the following mappings are used in our version of DES:

$EP:\mathbb{F}_2^{32} \rightarrow \mathbb{F}_2^{48}$: $EP\mathbf{x}$ is formed from $\mathbf{x}$ as follows: first $\mathbf{y}=P\mathbf{x}$ is formed by permuting the 32 bits of $\mathbf{x}$; then $EP\mathbf{x}=E\mathbf{y}$ is formed by taking 16 of the 32 bits of $\mathbf{y}$ once and the other 16 twice;

$S_j:\mathbb{F}_2^6 \rightarrow \mathbb{F}_2^4$ ($j=1, \cdots, 8$): the mappings defined by the S-boxes;

$S:\mathbb{F}_2^{48} \rightarrow \mathbb{F}_2^{32}: S(\mathbf{x}) = (S_1\mathbf{x}_1, \cdots, S_8\mathbf{x}_8)$ for $\mathbf{x}=(\mathbf{x}_1, \cdots, \mathbf{x}_8)$ with $\mathbf{x}_j \in \mathbb{F}_2^6$;

$L_i:\mathbb{F}_2^{56} \rightarrow \mathbb{F}_2^{48}$ ($i=1, \cdots, 16$): $L_i\mathbf{k} = PC2(C^{r(i)}\mathbf{k}_1, C^{r(i)}\mathbf{k}_2)$ for $\mathbf{k}=(\mathbf{k}_1,\mathbf{k}_2)$ with $\mathbf{k}_1,\mathbf{k}_2 \in \mathbb{F}_2^{28}$. Here $C\mathbf{x}$ is formed from $\mathbf{x}$ by applying a cyclic left shift to the bits of $\mathbf{x}$, $r(i)$ is an integer determined by the shift pattern in the NBS-description of the key-scheduling and $PC2(\mathbf{x},\mathbf{y})$ is formed from $\mathbf{x},\mathbf{y}$ by selecting 24 bits from $\mathbf{x}$, selecting 24 bits from $\mathbf{y}$ and permuting the selected 48 bits in some order.

The mappings EP, L_i are linear. If A is a linear mapping, then we say that A sends p to q if A maps the vector of which only the p-th bit is equal to 1 onto a vector of which at least the q-th bit equals 1. If A maps the vector with only a 1 in its p-th bit onto $\mathbf{0}$, we say that A does not choose p. Thus EP sends each p in $\{1, \cdots, 32\}$ to either one or two elements of $\{1, \cdots, 48\}$, while each p in $\{1, \cdots, 56\}$ is either not chosen by L_i or sent to exactly one element of $\{1, \cdots, 48\}$.

We shall now algebraically describe our version of DES. The message space is $\mathbb{F}_2^{64}$. Elements of $\mathbb{F}_2^{64}$ will be written in the form $(\mathbf{x},\mathbf{y})$, where $\mathbf{x},\mathbf{y} \in \mathbb{F}_2^{32}$. The key space is $\mathbb{F}_2^{56}$.

The mappings $F_i : \mathbb{F}_2^{64} \times \mathbb{F}_2^{56} \to \mathbb{F}_2^{64}$ $(i=1, \cdots, 16)$ (the "rounds") are defined by

$$F_i(\mathbf{q}_0,\mathbf{q}_1,\mathbf{k}) = (\mathbf{q}_1, \mathbf{q}_0 + S(EP\mathbf{q}_1 + L_i\mathbf{k})\ ) \quad \text{for } (\mathbf{q}_0,\mathbf{q}_1) \in \mathbb{F}_2^{64}, \mathbf{k} \in \mathbb{F}_2^{56}$$

and $DES : \mathbb{F}_2^{64} \times \mathbb{F}_2^{56} \to \mathbb{F}_2^{64}$ is defined by

$$DES = F_{16}F_{15} \cdots F_1.$$

Thus if $\mathbf{q}_2, \mathbf{q}_3, \cdots$ are defined by the recurrence sequence

$$\mathbf{q}_{i+1} = \mathbf{q}_{i-1} + S(EP\mathbf{q}_i + L_i\mathbf{k}) \quad (i=1, \cdots, 16)$$

then $DES(\mathbf{q}_0,\mathbf{q}_1,\mathbf{k}) = (\mathbf{q}_{16},\mathbf{q}_{17})$.

Let R, T be integers with $1 \leqslant R \leqslant T \leqslant 16$. We define

$$DES_{R,T} = F_T F_{T-1} \cdots F_R,$$
$$DES_{R,T}^{-1} = F_R^{-1} F_{R+1}^{-1} \cdots F_T^{-1}.$$

Let R, M, T be integers with $1 \leqslant R \leqslant M \leqslant T \leqslant 16$. For $\mathbf{p},\mathbf{c} \in \mathbb{F}_2^{64}, \mathbf{k} \in \mathbb{F}_2^{56}$, we put

$$\left.\begin{array}{l} \mathbf{d}' = d'_1 \cdots d'_{64} = DES_{R,M}(\mathbf{p},\mathbf{k}) , \\ \mathbf{d}'' = d''_1 \cdots d''_{64} = DES_{M+1,T}^{-1}(\mathbf{c},\mathbf{k}) , \\ \mathbf{k} = k_1 \cdots k_{56} . \end{array}\right\} \tag{14}$$

Our aim is to find out if there are subsets $\{i_1, \cdots, i_{64}\}$, $\{j_1, \cdots, j_r\}$ of $\{1, \cdots, 56\}$,$\{1, \cdots, 64\}$ respectively, such that $d'_{j_1}, \cdots, d'_{j_r}, d''_{j_1}, \cdots, d''_{j_r}$ are functionally independent of the key bits k_i with i different from $i_1, \cdots, i_s$.

Let $\mathbf{p},\mathbf{c}$ have the same meaning as above and put $\mathbf{p} = (\mathbf{q}_{R-1},\mathbf{q}_R)$,$\mathbf{c} = (\mathbf{q}'_T,\mathbf{q}'_{T+1})$. Define the sequences $\mathbf{q}_{R-1},\mathbf{q}_R,\mathbf{q}_{R+1}, \cdots, \mathbf{q}'_{T+1},\mathbf{q}'_T,\mathbf{q}'_{T-1}, \cdots$ by

$$\mathbf{q}_{i+1} = \mathbf{q}_{i-1} + S(EP\mathbf{q}_i + L_i\mathbf{k}) \ (i = R, R+1, \cdots) ,$$
$$\mathbf{q}'_{i-1} = \mathbf{q}'_{i+1} + S(EP\mathbf{q}'_i + L_i\mathbf{k}) \ (i = T, T-1, \cdots).$$

Let $t \in \{1, \cdots, 56\}$. We define the sets $X_i(t)$ $(i = R-1, R, R+1, \cdots)$, $X'_i(t)$ $(i = T+1, T, T-1, \cdots)$ recursively as follows:

$$\left.\begin{array}{l} X_{R-1}(t) = X_R(t) = \varnothing \;;\; X'_{T+1}(t) = X'_T(t) = \varnothing \;; \\ X_{i+1}(t) \text{ is the set of indices of the bits of } \mathbf{q}_{i+1} \text{ which functionally depend on} \\ \text{some of the bits of } \mathbf{q}_i \text{ with indices in } X_i(t)\text{, some of the bits of } \mathbf{q}_{i-1} \text{ with} \\ \text{indices in } X_{i-1}(t) \text{ and eventually } k_t; \\ X'_{i-1} \text{ is defined similarly in terms of } X'_i, X'_{i-1}, k_t. \end{array}\right\} \qquad (15)$$

Obviously, the sets of bits of $\mathbf{q}_i$, $\mathbf{q}'_i$ respectively, which are functionally dependent on k_t are included in $X_i(t), X'_i(t)$, respectively. An equivalent formulation of Meyer's assumption mentioned in §1 is that *all* indices in $X_i(t), X'_i(t)$ are of bits of $\mathbf{q}_i, \mathbf{q}'_i$ which are functionally dependent on k_t. For each t, we shall recursively compute the sets $X_i(t), X'_i(t)$. To this end, we introduce the following sets:

$$\begin{array}{lll} U_1 = \{1, 2, \cdots, 6\}, & U_2 = \{7, \cdots, 12\}, & \ldots, \; U_8 = \{43, \cdots, 48\}, \\ V_1 = \{1, 2, 3, 4\}, & V_2 = \{5, \cdots, 8\}, & \cdots, \; V_8 = \{29, \cdots, 32\}. \end{array}$$

Put $W_i(t) = \varnothing$ if L_i does not choose t and $W_i(t) = \{j\}$ if L_i sends t to an element of U_j. Finally, let $\mathcal{F}$ be a function, mapping subsets of $\{1, \cdots, 8\}$ onto subsets of $\{1, \cdots, 8\}$ which is defined as follows: $\mathcal{F}(A)$ is the set of integers j with the property that there is an $i \in A$ such that EP sends an element of V_i to an element of U_j. In particular, $\mathcal{F}(\varnothing) = \varnothing$.

$\mathcal{F}(\{1\}) = \{2,3,4,5,6,8\}$	$\mathcal{F}(\{5\}) = \{1,2,3,4,6,7\}$	
$\mathcal{F}(\{2\}) = \{1,3,4,5,7,8\}$	$\mathcal{F}(\{6\}) = \{1,2,3,5,7,8\}$	$\mathcal{F}(\varnothing) = \varnothing$
$\mathcal{F}(\{3\}) = \{2,4,5,6,7,8\}$	$\mathcal{F}(\{7\}) = \{1,2,3,4,6,8\}$	$\mathcal{F}(A \cup B) = \mathcal{F}(A) \cup \mathcal{F}(B)$
$\mathcal{F}(\{4\}) = \{1,3,5,6,7,8\}$	$\mathcal{F}(\{8\}) = \{1,2,4,5,6,7\}$	

table 1: the function $\mathcal{F}$

We define the sets $V_{R-1}(t), V_R(t), V_{R+1}(t), \cdots, V'_{T+1}(t), V'_T(t), V'_{T-1}(t), \cdots$ recursively as follows:

$$\left.\begin{array}{l} V_{R-1}(t) = V_R(t) = \varnothing, \; V'_{T+1}(t) = V'_T(t) = \varnothing, \\ V_{i+1}(t) = V_{i-1}(t) \cup \mathcal{F}(V_i(t)) \cup W_i(t) \quad (i = R, R+1, \cdots), \\ V'_{i-1}(t) = V'_{i+1}(t) \cup \mathcal{F}(V'_i(t)) \cup W_i(t) \quad (i = T, T-1, \cdots). \end{array}\right\} \qquad (16)$$

Using that for each S-box in DES, all four output bits functionally depend on all six input bits, we obtain

$$X_i(t)=\bigcup_{j\in V_i(t)} V_j \ , \ X'_i(t)=\bigcup_{j\in V'_i(t)} V_j \ . \tag{17}$$

Hence the integers j in $\{1,\cdots,64\}$ such that at least one of the bits d'_j,d''_j (cf. (14)) depends on k_t belong to the set

$$Q(t)=X_M(t)\cup X'_M(t)\cup\left\{j>32\colon j-32\in X_{M+1}(t)\cup X'_{M+1}(t)\right\}. \tag{18}$$

It is very easy to compute the sets $Q(t)$, using the recurrence relations (16).For each subset I of $\{1,\cdots,56\}$, the set J of integers in $\{1,\cdots,64\}$ not belonging to any of the sets $Q(t)$ with $t\in I$ has the property that for $j\in J$, both d'_j,d''_j, are functionally independent of the k_i with $i\in I$. The examples for the sets I,J in the table below have been obtained by computing for each j the set of t such that $j\notin Q(t)$. $N=T-R+1$ denotes the number of consecutive rounds.

R	M	T	N	J	I	$\#I$
1	2	4	4	9,10,11,12	1,3,4,10,14,15,18,25,28,32, 35,38,41,42,44,48,49,52,56	19
1	2	4	4	41,42,43,44	5,9,13,19,20,23,24,26,27,30, 33,36,37,39,43,44,47,51,55	19
1	2	5	5	41,42,43,44	5,20,26,27,30,37,43,44,51	9
1	3	6	6	5,6,7,8	7,28	2
1	3	6	6	17,18,19,20	36,45	2
1	4	7	7	-	-	-
2	5	8	7	5,6,7,8,13,14,15,16	21	1

table 2

In the theorem below we state that non-empty sets I,J of the same type as in table 2 can not be found for blockciphers consisting of 8 or more consecutive rounds of DES.

Theorem 1 . *Suppose that R,T are integers with $R\geqslant 1, T\leqslant 16, T\geqslant R+7$. Then for every integer M with $R\leqslant M\leqslant T$ and for each t in $\{1,\cdots,56\}$, $Q(t)=\{1,\cdots,64\}$.*

Proof: Let t,M be integers with $1\leqslant t\leqslant 56, R\leqslant M\leqslant T$. The key scheduling of DES has the property that each integer in $\{1,\cdots,56\}$ is chosen by at least one of the mappings L_i,L_{i+1} for $i=\{1,\cdots,15\}$. This can be verified by using the fact that the only integers in $\{1,\cdots,56\}$ not chosen by *PC2* are 9,18,22,25,35,38,43,54. Hence if there is an integer not chosen by L_i and L_j then $r(i)-r(j)$ must be equal to the difference (mod 28) of two of the integers 9,18,22,25 or of two of the integers 35,38,43,54. But $r(i+1)-r(i)$ is either equal to 1 or 2 for $i=1,\cdots,16$. From the recurrence relations (16) we infer that the sets $V_{R+2}(t), V'_{T-2}(t)$ are non-empty. It is easy to check from table 1, that $\mathcal{F}^2$ ($\mathcal{F}$ iterated twice) maps each non-empty subset of $\{1, \cdots, 8\}$ onto $\{1, \cdots, 8\}$. Again by (16), we infer that $V_{R+4}(t) = V_{R+5}(t) = \cdots = \{1, \cdots, 8\}$, $V'_{T-4} = V'_{T-5} = ... = \{1, \cdots, 8\}$. We have either $M \geqslant R+4$, or $M+1 \leqslant T-4$, or $M+1 = R+4$ and $M = T-4$. In these three cases, we have $X_M(t) \bigcup X'_M(t) = X_{M+1}(t) \bigcup X'_{M+1}(t) = \{1, \cdots, 32\}$. This proves Theorem 1. □

Remark. By a similar method as in the proof of Theorem 1, one can show that in case $T = R+6$, $Q(t)$ can only be a proper subset of $\{1, \cdots, 64\}$ if t is not chosen by both L_R and L_T. From the shift-pattern one recovers that $r(R+6) - r(R)$ is equal to either 11 or 12 for $R = 1, 2, \cdots, 10$. If *PC2* is made in such a way that no difference of the integers not chosen by *PC2* is congruent to 1,2,11 or 12 (mod 28) then in Theorem 1 we can replace $R+7$ by $R+6$. We do not know if, by a proper choice of *PC2*, $R+7$ can be replaced by $R+5$.

4. SEQUENCES OF FACTOR SPACES IN DES

In this section we shall investigate the sequences of factor spaces in blockciphers consisting of a reduced number of rounds of DES . We shall use the same notation as in the previous sections. In particular, the blockciphers $F_i : \mathbb{F}_2^{64} \times \mathbb{F}_2^{56} \rightarrow \mathbb{F}_2^{64}$ are defined by $F_i(\mathbf{q}_0, \mathbf{q}_1, \mathbf{k}) = (\mathbf{q}_1, \mathbf{q}_0 + S(EP\mathbf{q}_1 + L_i\mathbf{k}))$ for $(\mathbf{q}_0, \mathbf{q}_1) \in \mathbb{F}_2^{64}$ and $\mathbf{k} \in \mathbb{F}_2^{56}$, and $DES_{R,T} = F_T F_{T-1} \cdots F_R$. We shall implicitly assume that the sequences of factor spaces we will consider are all with respect to $F_R, \cdots, F_T$. Our aim is to investigate if $DES_{R,T}$ has sequences of *useful* factor spaces. (A sequence of factor spaces $(\mathcal{V}_{R-1}, \mathcal{V}_R, \cdots, \mathcal{V}_T; \mathcal{W})$ is called useful if $\mathcal{W} \neq [\mathbf{0}]$ and $\mathcal{V}_T \neq \mathbb{F}_2^{64}$).

Example 1. Let t $\in \{1, \cdots, 56\}$ and let $X_{R-1}(t), X_R(t), \cdots$ be the sets recursively defined by (15). Let $\mathcal{V}_i$ be the spaces of vectors of which the bits with indices outside

$$Y_i(t) = X_i(t) \bigcup \left\{ j > 32 : j - 32 \in X_{i+1}(t) \right\}$$

are 0 and let $\mathcal{W}$ be the space generated by the vector in $\mathbb{F}_2^{56}$ of which only the t-th bit is equal to 1. Then $(\mathcal{V}_{R-1}, \mathcal{V}_R, \cdots, \mathcal{V}_T; \mathcal{W})$ is a sequence of factor spaces for $DES_{R,T}$ and this sequence is useful if and only if $Y_T(t)$ is properly contained in $\{1, \cdots, 64\}$.

Example 2. Reeds and Manferdelli [84] introduced the notion of a "per round linear factor" for DES. A per round linear factor is a linear mapping A on $\mathbb{F}_2^{48}$ for which there exist a mapping $\tilde{S}$ with $AEPS = \tilde{S}A$. If there exists a per round linear factor A which is neither invertible nor has the property that AE maps each vector to $\mathbf{0}$ then one can prove that $(\mathcal{V}, \cdots, \mathcal{V}; \mathcal{W})$ is a useful sequence of factor spaces for $DES_{R,T}$, where

$$\mathcal{V} = [(\mathbf{v}_0, \mathbf{v}_1) \in \mathbb{F}_2^{64} : AE\mathbf{v}_0 = AE\mathbf{v}_1 = \mathbf{0}] ,$$

$$\mathcal{W} = [\mathbf{k} \in \mathbb{F}_2^{56} : L_R\mathbf{k} = L_{R+1}\mathbf{k} = \cdots = L_T\mathbf{k} = \mathbf{0}] .$$

If $\mathcal{V},\mathcal{U}$ are subspaces of $\mathbb{F}_2^{64},\mathbb{F}_2^{48}$ respectively, then the spaces $S^P(\mathcal{V}),S^K(\mathcal{U})$ are defined by

$$S^P(\mathcal{V})=[(\mathbf{v}_1,\mathbf{v}_0+S(EP\mathbf{v}_1+\mathbf{c})+S(\mathbf{c})):(\mathbf{v}_0,\mathbf{v}_1)\in\mathcal{V},\mathbf{c}\in\mathbb{F}_2^{48}]\,,$$
$$S^K(\mathcal{U})=[(\mathbf{0},S(\mathbf{u}+\mathbf{c})+S(\mathbf{c})):\mathbf{u}\in\mathcal{U},\mathbf{c}\in\mathbb{F}_2^{48}]\,.$$

Lemma 2. *Let $\mathcal{V}_{R-1},\mathcal{V}_R,\cdots,\mathcal{V}_T\subseteq\mathbb{F}_2^{64},\mathcal{W}\subseteq\mathbb{F}_2^{56}$ be vector spaces. Then the following statements are equivalent:*

(i) $(\mathcal{V}_{R-1},\mathcal{V}_R,\cdots,\mathcal{V}_T;\mathcal{W})$ is a sequence of linear factors for $DES_{R,T}$;

(ii) $S^P(\mathcal{V}_{i-1})+S^K(L_i(\mathcal{W}))\subseteq\mathcal{V}_i$ for $i=R,R+1,\cdots,T$.

Proof: In view of Lemma 1, it suffices to show that for $i=R,R+1,\cdots,T$,

$$\begin{aligned}&S^P(\mathcal{V}_{i-1})+S^K(L_i(\mathcal{W}))=\\&[F_i(\mathbf{q}_0+\mathbf{v}_0,\mathbf{q}_1+\mathbf{v}_1,\mathbf{k}+\mathbf{w})+F_i(\mathbf{q}_0,\mathbf{q}_1,\mathbf{k}):\ (\mathbf{q}_0,\mathbf{q}_1)\in\mathbb{F}_2^{64},\mathbf{k}\in\mathbb{F}_2^{56},(\mathbf{v}_0,\mathbf{v}_1)\in\mathcal{V},\mathbf{w}\in\mathcal{W}]\,.\end{aligned}\tag{19}$$

Denote the right-hand side of (19) by $\mathcal{W}_i$. Let $i\in\{R,\cdots,T\}$. It is easy to check that for $(\mathbf{v}_0,\mathbf{v}_1)\in\mathcal{V},\mathbf{c}\in\mathbb{F}_2^{48}$,

$$(\mathbf{v}_1,\mathbf{v}_0+S(EP\mathbf{v}_1+\mathbf{c})+S(\mathbf{c})=F_i(\mathbf{v}_0,\mathbf{v}_1,\mathbf{k})+F_i(\mathbf{0},\mathbf{0},\mathbf{k}),$$

where $\mathbf{k}\in\mathbb{F}_2^{56}$ is chosen such that $L_i\mathbf{k}=\mathbf{c}$. This shows that

$$S^P(\mathcal{V}_{i-1})\subseteq\mathcal{W}_i.\tag{20}$$

It is also easy to verify that for $\mathbf{w}\in\mathcal{W},\mathbf{c}\in\mathbb{F}_2^{48}$,

$$(\mathbf{0},S(L_i\mathbf{w}+\mathbf{c})+S(\mathbf{c}))=F_i(\mathbf{0},\mathbf{0},\mathbf{k}+\mathbf{w})+F_i(\mathbf{0},\mathbf{0},\mathbf{k}),$$

where again $\mathbf{k}\in\mathbb{F}_2^{56}$ is chosen such that $L_i\mathbf{k}=\mathbf{c}$. Hence

$$S^K(L_i(\mathcal{W}))\subseteq\mathcal{W}_i.\tag{21}$$

On the other hand, for $(\mathbf{q}_0,\mathbf{q}_1)\in\mathbb{F}_2^{64},\mathbf{k}\in\mathbb{F}_2^{56},(\mathbf{v}_0,\mathbf{v}_1)\in\mathcal{V}_{i-1},\mathbf{w}\in\mathcal{W}$,

$$\begin{aligned}&F_i(\mathbf{q}_0+\mathbf{v}_0,\mathbf{q}_1+\mathbf{v}_1,\mathbf{k}+\mathbf{w})+F_i(\mathbf{q}_0,\mathbf{q}_1,\mathbf{k})\\&\quad=(\mathbf{v}_1,\mathbf{v}_0+S(EP\mathbf{v}_1+L_i\mathbf{w}+EP\mathbf{q}_1+L_i\mathbf{k})+S(EP\mathbf{q}_1+L_i\mathbf{k}))\\&\quad=(\mathbf{v}_1,\mathbf{v}_0+S(EP\mathbf{v}_1+\mathbf{c}_1)+S(\mathbf{c}_1))+(\mathbf{0},S(L_i\mathbf{w}+\mathbf{c}_2)+S(\mathbf{c}_2)),\end{aligned}$$

where

$$\mathbf{c}_1=L_i\mathbf{w}+EP\mathbf{q}_1+L_i\mathbf{k}\ ,\ \ \mathbf{c}_2=EP\mathbf{q}_1+L_i\mathbf{k}\,.$$

Hence

$$\mathcal{W}_i \subseteq S^P(\mathcal{V}_{i-1}) + S^K(L_i(\mathcal{W})). \tag{22}$$

A combination of (20),(21),(22) yields (19). □

In the statement of the next lemma, we use the following notation. Define the linear mappings $\rho_i:\mathbb{F}_2^{48}\to\mathbb{F}_2^{6}$, $\rho_i^*:\mathbb{F}_2^{4}\to\mathbb{F}_2^{32}$, $\rho_i^{**}:\mathbb{F}_2^{4}\to\mathbb{F}_2^{64}$, $U:\mathbb{F}_2^{64}\to\mathbb{F}_2^{48}$ as follows:

$\rho_i(\mathbf{x})=\mathbf{x}_i$ for $\mathbf{x}=(\mathbf{x}_1,\cdots,\mathbf{x}_8)$ with $\mathbf{x}_1,\cdots,\mathbf{x}_8\in\mathbb{F}_2^6$;
$\rho_i^*(\mathbf{y})=(\mathbf{0},\cdots,\mathbf{0},\mathbf{y},\mathbf{0},\cdots,\mathbf{0})$ (with $\mathbf{y}$ on the i-th place) ;
$\rho_i^{**}(\mathbf{y})=(\mathbf{0},\rho_i^*(\mathbf{y}))$;
$U(\mathbf{x},\mathbf{y})=EP\mathbf{y}$.

Finally, for any subspace $\mathcal{U}$ of $\mathbb{F}_2^6$, we define the spaces $T_j(\mathcal{U}),T'_j(\mathcal{U})$ $(j=1,\cdots,8)$ by

$$T_j(\mathcal{U})=[S_j(\mathbf{u}+\mathbf{c})+S_j(\mathbf{c}):\mathbf{u}\in\mathcal{U},\mathbf{c}\in\mathbb{F}_2^6]\,,$$
$$T'_j(\mathcal{U})=[S_j(\mathbf{u}+\mathbf{c})+S_j(\mathbf{c})+S_j(\mathbf{u})+S_j(\mathbf{0}):\mathbf{u}\in\mathcal{U},\mathbf{c}\in\mathbb{F}_2^6]\,.$$

Lemma 3. *Let* $\mathcal{V}=[(\mathbf{v}_{0j},\mathbf{v}_{1j}):j=1,\cdots,p]\subseteq\mathbb{F}_2^{64}$, $\mathcal{W}=[\mathbf{w}_j:j=1,\cdots,q]\subseteq\mathbb{F}_2^{48}$ *be vector spaces. Then*

$$S^P(\mathcal{V})=[(\mathbf{v}_{1j},\mathbf{v}_{0j}+S(EP\mathbf{v}_{1j})+S(\mathbf{0})):\, j=1,\cdots,p] + \sum_{k=1}^{8}\rho_k^{**}T'_k\{\rho_k U(\mathcal{V})\} \tag{23}$$

and

$$S^K(\mathcal{W})=[(\mathbf{0},S(\mathbf{w}_j)+S(\mathbf{0})):j=1,\cdots,q] + \sum_{k=1}^{8}\rho_k^{**}T'_k\{\rho_k(\mathcal{W})\}. \tag{24}$$

Proof: We shall only prove (23); (24) can be proved in a similar way. For convenience, we introduce the following notation:

$\mathbf{s}(\mathbf{v}_0,\mathbf{v}_1,\mathbf{c})=(\mathbf{v}_1,\mathbf{v}_0+S(EP\mathbf{v}_1+\mathbf{c})+S(\mathbf{c}))$ for $(\mathbf{v}_0,\mathbf{v}_1)\in\mathbb{F}_2^{64},\mathbf{c}\in\mathbb{F}_2^{48}$;
$\mathbf{t}'_j(\mathbf{u},\mathbf{c})=S_j(\mathbf{u}+\mathbf{c})+S_j(\mathbf{c})+S_j(\mathbf{u})+S_j(\mathbf{0})$ for $\mathbf{u},\mathbf{c}\in\mathbb{F}_2^6$.

First of all we remark, that for subspaces $\mathcal{V}_1,\mathcal{V}_2$ of $\mathbb{F}_2^{64}$,

$$S^P(\mathcal{V}_1+\mathcal{V}_2)=S^P(\mathcal{V}_1)+S^P(\mathcal{V}_2) \tag{25}$$

and that for subspaces $\mathcal{U}_1, \mathcal{U}_2$ of $\mathbb{F}_2^6$,

$$T'_j(\mathcal{U}_1 + \mathcal{U}_2) = T'_j(\mathcal{U}_1) + T'_j(\mathcal{U}_2) \text{ for } j = 1, \cdots, 8. \tag{26}$$

(25) follows easily from the identity

$$\mathbf{s}(\mathbf{v}'_0 + \mathbf{v}''_0, \mathbf{v}'_1 + \mathbf{v}''_1, \mathbf{c}) = \mathbf{s}(\mathbf{v}'_0, \mathbf{v}'_1, \mathbf{c} + EP\mathbf{v}''_1) + \mathbf{s}(\mathbf{v}''_0, \mathbf{v}''_1, \mathbf{c})$$
$$\text{for } (\mathbf{v}'_0, \mathbf{v}''_1), (\mathbf{v}''_0, \mathbf{v}''_1) \in \mathbb{F}_2^{64}, \mathbf{c} \in \mathbb{F}_2^{48},$$

while (26) is an easy consequence of the identity

$$\mathbf{t}'_j(\mathbf{u}' + \mathbf{u}'', \mathbf{c}) = \mathbf{t}'_j(\mathbf{u}', \mathbf{u}'' + \mathbf{c}) + \mathbf{t}'_j(\mathbf{u}'', \mathbf{c}) + \mathbf{t}'_j(\mathbf{u}', \mathbf{u}'')$$
$$\text{for } \mathbf{u}', \mathbf{u}'', \mathbf{c} \in \mathbb{F}_2^6, \ j = 1, \cdots, 8.$$

In view of (25),(26), it suffices to prove (23) for p = 1. Let $\mathcal{V} = [(\mathbf{v}_0, \mathbf{v}_1)]$ and put

$$\tilde{\mathcal{V}} = [(\mathbf{v}_1, \mathbf{v}_0 + S(EP\mathbf{v}_1) + S(\mathbf{0})] = [\mathbf{s}(\mathbf{v}_0, \mathbf{v}_1, \mathbf{0})],$$
$$\tilde{\mathcal{U}}_j = \rho_j^{**} T'_j\{\rho_j U([\mathbf{v}_1])\} = [\rho_j^{**} \mathbf{t}'_j(\rho_j EP\mathbf{v}_1, \mathbf{c}) : \mathbf{c} \in \mathbb{F}_2^6] \text{ for } j = 1, \cdots, 8.$$

From the identity

$$\mathbf{s}(\mathbf{v}_0, \mathbf{v}_1, \mathbf{c}) = \mathbf{s}(\mathbf{v}_0, \mathbf{v}_1, \mathbf{0}) + \sum_{k=1}^{8} \rho_k^{**} \mathbf{t}'_k(\rho_k EP\mathbf{v}_1, \rho_k \mathbf{c}) \quad \text{for } \mathbf{c} \in \mathbb{F}_2^{48}, \tag{27}$$

it follows easily that

$$S^P(\mathcal{V}) \subseteq \tilde{\mathcal{V}} + \sum_{k=1}^{8} \tilde{\mathcal{U}}_k. \tag{28}$$

On the other hand we have

$$\tilde{\mathcal{V}} \subseteq S^P(\mathcal{V}). \tag{29}$$

Let $\mathbf{d} \in \mathbb{F}_2^6$ and choose $\mathbf{c} \in \mathbb{F}_2^{48}$ such that $\rho_j(\mathbf{c}) = \mathbf{d}, \rho_k(\mathbf{c}) = \mathbf{0}$ for $k \neq j$. Then (27) implies that

$$\rho_j^{**} \mathbf{t}'_j(\rho_k EP_{\mathbf{v}_1}, \mathbf{d}) = \mathbf{s}(\mathbf{v}_0, \mathbf{v}_1, \mathbf{c}) + \mathbf{s}(\mathbf{v}_0, \mathbf{v}_1, \mathbf{0}).$$

Hence

$$\tilde{\mathcal{U}}_j \subseteq S^P(\mathcal{V}) \text{ for } j = 1, \cdots, 8. \tag{30}$$

Now (23) follows at once from (28),(29),(30). □

Lemma 3 shows that for each subspace $\mathcal{V}$ of $\mathbb{F}_2^{64}$ ($\mathcal{W}$ of $\mathbb{F}_2^{56}$) the space $S^P(\mathcal{V})$,$(S^K(\mathcal{W}))$ can be expressed as the sum of a space generated by a set of vectors of which the cardinality is not larger than the dimension of $\mathcal{V}$ ($\mathcal{W}$) and spaces which can be described completely in terms of the S-boxes. Thus Lemma 3 provides us a rather efficient method which checks if a given sequence of spaces $(\mathcal{V}_{R-1},\mathcal{V}_R, \cdots ,\mathcal{V}_T,\mathcal{W})$ is a sequence of factor spaces for $DES_{R,T}$. From the arguments used in the proof of Lemma 3 it is clear, that this method can be applied also to a general class of block ciphers which can be described in the same way as DES, with arbitrary S-boxes (which can be different in each round), an arbitrary linear mapping instead of EP (where it is allowed that in different rounds different linear mappings are chosen) and arbitrary surjective linear mappings instead of the L_i.

We shall now give explicit expressions for the spaces $S^P(\mathcal{V})$, $S^K(\mathcal{W})$. For this purpose we have only to compute the spaces $T'(\mathcal{U})$ with $\mathcal{U} \subseteq \mathbb{F}_2^6$.

Lemma 4. *For all g in $\{1, \cdots ,8\}$ and all subspaces $\mathcal{U}$ of $\mathbb{F}_2^6$ with $\mathcal{U}\neq[\mathbf{0}]$, we have $T_g(\mathcal{U})=T'_g(\mathcal{U})=\mathbb{F}_2^4$, with the following exceptions:*

$T_4([000001])=[1100,0011,1010]$,$T'_4([000001])=[1100,0011]$;
$T_4([101110])=T'_4([101110])=[1010,0101]$;
$T_4([101111])=T'_4([101111])=[1001,0110]$;
$T_4([000001,101110])=T'_4([000001,101110])=[1100,0011,1010]$.

Proof: This can be verified by straightforward computation. □

In the theorem below, the sets $\mathbb{S}^P(\mathcal{V})$,$\mathbb{S}^K(\mathcal{W})$, with $\mathcal{V}$,$\mathcal{W}$ being subspaces of $\mathbb{F}_2^{64}$,$\mathbb{F}_2^{48}$ respectively, are defined by

$$\mathbb{S}^P(\mathcal{V})=\{g:1\leqslant g\leqslant 8,\ \rho_g U(\mathcal{V})\neq[\mathbf{0}]\ \},$$
$$\mathbb{S}^K(\mathcal{W})=\{g:1\leqslant g\leqslant 8,\ \rho_g(\mathcal{W})\neq[\mathbf{0}]\ \}.$$

Theorem 2. *Let $\mathcal{V}$,$\mathcal{W}$ be subspaces of $\mathbb{F}_2^{64}$,$\mathbb{F}_2^{48}$ respectively. Then*

$$(i)\quad S^P(\mathcal{V})=\tilde{\mathcal{V}}+\sum_{g\in\mathbb{S}^P(\mathcal{V})}\mathcal{V}_g,$$

where

$$\tilde{\mathcal{V}}=[(\mathbf{v}_1,\mathbf{v}_0)]:(\mathbf{v}_0,\mathbf{v}_1)\in\mathcal{V}]\quad \textit{if}\ \rho_4 U(\mathcal{V})\neq[000001]\ ,$$

$$\tilde{\mathcal{V}}=\left[(\mathbf{v}_1,\mathbf{v}_0+\alpha\rho_4^*(1010)):\ (\mathbf{v}_0,\mathbf{v}_1)\in\mathcal{V},\ \begin{cases}\alpha=0\ \textit{if}\ \rho_4 EP\mathbf{v}_1=000000\\ \alpha=1\ \textit{if}\ \rho_4 EP\mathbf{v}_1=000001\end{cases}\right]$$

if $\rho_4 U(\mathcal{V})=[000001]$;

and where

$$\mathcal{V}_g=\rho_g^{**}\mathbb{F}_2^4 \textit{ for } g\in\mathbb{S}^P(\mathcal{V})$$

with the following exceptions if $4\in\mathbb{S}^P(\mathcal{V})$*:*

$$\mathcal{V}_4=\rho_4^{**}([1100,0011]) \textit{ if } \rho_4 U(\mathcal{V})=[000001] ;$$
$$\mathcal{V}_4=\rho_4^{**}([1010,0101]) \textit{ if } \rho_4 U(\mathcal{V})=[101110] ;$$
$$\mathcal{V}_4=\rho_4^{**}([1001,0110]) \textit{ if } \rho_4 U(\mathcal{V})=[101111] ;$$
$$\mathcal{V}_4=\rho_4^{**}([1100,0011,1010]) \textit{ if } \rho_4 U(\mathcal{V})=[000001,101110] .$$

(ii) $S^K(\mathcal{W})=\sum\limits_{g\in\mathbb{S}^K(\mathcal{W})}\mathcal{W}_g$,

where $\mathcal{W}_g=\rho_g^{**}\mathbb{F}_2^4$ *for* $g\in\mathbb{S}^K(\mathcal{W})$ *with the following exceptions if* $4\in\mathbb{S}^K(\mathcal{W})$*:*

$$\mathcal{W}_4=\rho_4^{**}([1010,0101]) \textit{ if } \rho_4(\mathcal{W})=[101110] ;$$
$$\mathcal{W}_4=\rho_4^{**}([1001,0110]) \textit{ if } \rho_4(\mathcal{W})=[101111] ;$$
$$\mathcal{W}_4=\rho_4^{**}([1100,0011,1010]) \textit{ if } \rho_4(\mathcal{W})=[000001] \textit{ or } [000001,101110] .$$

Proof: The proofs of (i),(ii) can be derived easily from Lemmas 3,4. We shall only give a rough sketch of the proof of (i). By Lemma 4,

$$\rho_g^{**}\left[S_g(\rho_g\mathbf{v}_1)+S_g(\mathbf{0})\right]\in\mathcal{V}_g \quad \text{for } g\in\mathbb{S}^P(\mathcal{V})$$

except when $g=4$, $\rho_4 EP\mathbf{v}_1=000001$. This proves that for $(\mathbf{v}_0,\mathbf{v}_1)\in\mathcal{V}$, there is a vector $\mathbf{u}\in\sum\limits_{g\in\mathbb{S}^P(\mathcal{V})}\mathcal{V}_g$, with

$$(\mathbf{v}_1,\mathbf{v}_0+S(EP\mathbf{v}_1)+S(\mathbf{0}))=(\mathbf{v}_1,\mathbf{v}_0+\mathbf{u}) \ \text{ if } \rho_4 EP\mathbf{v}_1\neq 000001 ,$$

$$\begin{aligned}(\mathbf{v}_1,\mathbf{v}_0+S(EP\mathbf{v}_1)+S(\mathbf{0})) &= \\ &= \left[\mathbf{v}_1,\mathbf{v}_0+\rho_4^{**}\{S_4(\rho_4 EP\mathbf{v}_1)+S_4(\mathbf{0})\}\right]+\mathbf{u} \\ &= \left[\mathbf{v}_1,\mathbf{v}_0+\rho_4^{**}(1010)\right]+\mathbf{u}\end{aligned}$$

if $\rho_4 EP\mathbf{v}_1=000001.$

These facts immediately prove (i). □

We shall now prove that blockciphers consisting of eight or more consecutive rounds of DES are resistant against a meet-in-the-middle attack using sequences of factor spaces. To this end we shall need the following lemma.

Lemma 5. *Let* $T \geqslant R+3$. *If* $(\mathcal{V}_{R-1}, \mathcal{V}_R, \cdots, \mathcal{V}_T; \mathcal{W})$ *is a sequence of factor spaces for* $DES_{R,T}$ *with* $\mathcal{W} \neq [\mathbf{0}]$, *then*

(*i*) $\mathcal{V}_{R+3} \supseteq [(\mathbf{0},\mathrm{y}):\mathrm{y} \in \mathbb{F}_2^{32}]$,
(*ii*) $\mathcal{V}_{R+i} = \mathbb{F}_2^{64}$ for $i \geqslant 4$.

Proof: (ii) is an immediate consequence of (i) and Lemmas 2,4. We shall now prove (i). Since all elements of $\{1, \cdots, 56\}$ are chosen by at least one of the mappings L_R, L_{R+1}, at least one of the spaces $S^K(L_R(\mathcal{W})), S^K(L_{R+1}(\mathcal{W}))$ is $\neq [\mathbf{0}]$. By Lemma 2 and Theorem 2,

$$\mathcal{V}_{R+1} \supseteq \sum_{g \in \mathbb{S}} \mathcal{V}_g^1$$

for some non-empty subset $\mathbb{S}$ of $\{1, \cdots, 8\}$, where $\mathcal{V}_g^1 = \rho_g^{**}(\mathbb{F}_2^4)$ if $g \neq 4$ and $\mathcal{V}_4^1 = \rho_4^{**}(\mathcal{U}^1)$ with $\mathcal{U}^1$ being a subspace of $\mathbb{F}_2^4$ with $\mathcal{U} \neq [\mathbf{0}]$ in case that $4 \in \mathbb{S}$. The space $\mathcal{U}^1$ has the property that for each j in $\{1, \cdots, 4\}$ there is a vector $x_1x_2x_3x_4$ in $\mathcal{U}^1$ with $x_j \neq 0$. *EP* sends the indices of the output bits of S-box S_j (i.e the elements of $\{4j-3, \cdots, 4j\}$) to the indices of the input bits of 6 different S-boxes, namely the S-boxes S_k with $k \in \mathcal{F}(\{j\})$, where $\mathcal{F}$ is the function defined in table 1. Together with Lemma 2 and Theorem 2 these facts imply that

$$\mathcal{V}_{R+2} \supseteq \sum_{g \in \mathcal{F}(\mathbb{S})} \mathcal{V}_g^2,$$

where $\mathcal{V}_g^2 = \rho_g^{**}(\mathbb{F}_2^4)$ for $g \neq 4$ and when $4 \in \mathcal{F}(\mathbb{S})$, $\mathcal{V}_4^2 = \rho_g^{**}(\mathcal{U}^2)$ for some subspace $\mathcal{U}^2$ of $\mathbb{F}_2^4$ with $\mathcal{U}^2 \neq [\mathbf{0}]$. We remark that

$$S^P(\rho_g^{**}(\mathbb{F}_2^4)) \supseteq \rho_4^{**}(\mathbb{F}_2^4) \text{ for } g = 2,3,5,7,8, \tag{31}$$

hence $\mathcal{U}^2 = \mathbb{F}_2^4$ if one of the numbers 2,3,5,7,8 belongs to $\mathbb{S}$. Since $\mathcal{F}(\mathbb{S})$ has cardinality at least 6, at least one of the numbers 2,3,5,7,8 belongs to $\mathcal{F}(\mathbb{S})$. By repeating the argument from above, and using that $\mathcal{F}^2$ maps each non-empty subset of $\{1, \cdots, 8\}$ onto $\{1, \cdots, 8\}$, we obtain

$$\mathcal{V}_{R+3} \supseteq \sum_{g \in \mathcal{F}^2(\mathbb{S})} \rho_g^{**}(\mathbb{F}_2^4) = [(\mathbf{0},\mathrm{y}):\mathrm{y} \in \mathbb{F}_2^{32}].$$

This completes the proof of Lemma 5. □

Lemma 5 includes the result of Meyer mentioned in §1. Another consequence of Lemma 5 is that the only per round linear factors of DES are the linear mappings $A: \mathbb{F}_2^{48} \to \mathbb{F}_2^{48}$ for which either A is invertible or AE maps each vector of $\mathbb{F}_2^{32}$ onto $\mathbf{0}$. (cf. example 2 at the beginning of this section.) This fact was already proved by Reeds and Manferdelli [84].

We shall now prove our final result.

Theorem 3. *Let R,M,T be integers with $1 \leqslant R \leqslant M \leqslant T \leqslant 16$ and $T \geqslant R+7$. Let $(\mathcal{V}_{R-1}, \mathcal{V}_R, \cdots, \mathcal{V}_M; \mathcal{W})$, $(\mathcal{V}'_T, \mathcal{V}'_{T-1}, \cdots, \mathcal{V}'_M; \mathcal{W})$ be sequences of factor spaces for $DES_{R,M}, DES^{-1}_{M+1,T}$, respectively, such that $\mathcal{W} \neq [\mathbf{0}]$ and $\mathcal{V}_M = \mathcal{V}'_M$. Then*

$$\mathcal{V}_M = \mathcal{V}'_M = \mathbb{F}_2^{64}.$$

Proof: In the proof we shall use that the inverse of a round of DES (i.e. one of the blockciphers F_i) is equal to the round itself, except that the left half and the right half of both plaintext and ciphertext must be interchanged.

We distinguish three cases: (i) $M \geqslant R+4$; (ii) $M \leqslant T-5$; (iii) $M=R+3=T-4$. In case (i) we have $\mathcal{V}_M = \mathbb{F}_2^{64}$, by Lemma 5, (ii). In case (ii) we can prove, completely similar to Lemma 5, (ii), that $\mathcal{V}_M = \mathbb{F}_2^{64}$, using that all elements of $\{1, \cdots, 56\}$ are chosen by at least one of the mappings L_T, L_{T-1}. In case (iii) we have firstly, by Lemma 5,(i), $\mathcal{V}_M = \mathcal{V}_{R+3} \supseteq [(\mathbf{0},\mathrm{y}):\mathrm{y} \in \mathbb{F}_2^{32}]$. By an argument completely similar to the proof of Lemma 5 (i), one has $\mathcal{V} = \mathcal{V}'_{T-4} \supseteq [(\mathrm{x},\mathbf{0}):\mathrm{x} \in \mathbb{F}_2^{32}]$. This completes the proof of Theorem 3. □

Remark. By changing *PC2* in the way described at the end of §3, it is possible to replace the condition $T \geqslant R+7$ by $T \geqslant R+6$ in Theorem 3. This can be proved in a similar way as Theorem 3.

CONCLUDING REMARKS

Linear structures allowing known-plaintext attacks on blockciphers have been investigated, particularly those consisting of a reduced number of consecutive rounds of DES. The first structures we looked for were "bits in the middle" independent of key bits. Such independencies were found only in blockciphers comprising less than eight rounds of DES. We discovered that $PC2$ was not optimal in the sense that by a change of $PC2$ blockciphers of seven instead of eight consecutive rounds of DES would have no "bits in the middle" independent of key bits. The existence of such independencies in blockciphers for such numbers of rounds depends only on the structure of the tables E, P, and $PC2$; these independencies would hold for any S-boxes. More general linear structures were also considered, namely sequences of linear factors. The existence of these factors depends not only on the structure of E, P, and $PC2$, but also on the structure of the S-boxes. In spite of some linear structure in S-box 4, we were able to show that blockciphers consisting of eight or more consecutive rounds of DES do not have sequences of linear factors with respect to these rounds that can reduce the search time for the key in a meet-in-the-middle attack.

A natural extension of the attacks described in this paper would seek changes in the tables defining the S-boxes that yield S-boxes with linear factors cooperating to give useful sequences of linear factors. (One might even change the S-boxes differently in different rounds.) Any sequence of linear factors for the cipher with the modified S-boxes is then a sequence of "near" linear factors for the original cipher. (As has been pointed out in §2, such attacks generalize several ideas in [Hellman et al 76] and [Desmedt, Quisquater and Davio 84].) In this way one might obtain sequences of near linear factors that allow cryptanalysis of blockciphers consisting of eight or more rounds of DES.

REFERENCES

(1) National Bureau of Standards, "Data Encryption Standard", U.S. Department of Commerce, FIPS pub. 46 (January 1977).

(2) Davio, M., Desmedt, Y., Fosséprez, 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) Desmedt, Y., Quisquater, J.J., Davio, M., "Dependence of output on input in DES: Small avalanche characteristics," in Advances in Cryptology: Proc. Crypto '84, G.R. Blakley and D. Chaum, eds., Lecture Notes in Computer Science 196, Springer-Verlag, Berlin (1985), pp. 359-376.

(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) 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 (1985), pp. 377-389.