# Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers

Kenneth G. Paterson
Extended Enterprise Laboratory
HP Laboratories Bristol
HPL-1999-12
January, 1999

E-mail: kp@hplb.hpl.hp.com

block, cipher, trapdoor, cryptanalysis, linear, differential, permutation, group

An iterated block cipher can be regarded as a means of producing a set of permutations of a message space. Some properties of the group generated by the round functions of such a cipher are known to be of cryptanalytic interest. It is shown here that if this group acts imprimitively on the message space then there is an exploitable weakness in the cipher. It is demonstrated that a weakness of this type can be used to construct a trapdoor that appears to be difficult to detect. An example of a DES-like cipher, resistant to both linear and differential cryptanalysis that generates an imprimitive group and is easily broken, is given. Some implications for block cipher design are noted.

Internal Accession Date Only

# Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers

Kenneth G. Paterson*

Hewlett-Packard Laboratories,
Filton Rd., Stoke Gifford,
Bristol BS34 8QZ, U.K.
kp@hplb.hpl.hp.com

**Abstract.** An iterated block cipher can be regarded as a means of producing a set of permutations of a message space. Some properties of the group generated by the round functions of such a cipher are known to be of cryptanalytic interest. It is shown here that if this group acts imprimitively on the message space then there is an exploitable weakness in the cipher. It is demonstrated that a weakness of this type can be used to construct a trapdoor that appears to be difficult to detect. An example of a DES-like cipher, resistant to both linear and differential cryptanalysis that generates an imprimitive group and is easily broken, is given. Some implications for block cipher design are noted.

## 1 Introduction

An iterated block cipher can be regarded as a means of producing a set of permutations of a message space by the repetition of simpler round functions. Properties of the groups generated by the round functions and by the actual encryptions of such a cipher have long been recognised as having cryptographic importance. For example, if either of these groups is "small" in size then the cipher may be regarded as having a weakness, since not every possible permutation of the message space can be realised by the cipher, [6, 8]. Moreover, multiple encryption may offer little or no additional security if these groups are small. Attacks on ciphers whose encryptions generate small groups were given in [12].

Naturally, much attention has been devoted to groups associated with the DES. Early studies in [6] and [8] concentrated on the groups generated by a set of "DES-like functions", of which the actual round functions of the DES form a subset. It was shown that these functions can generate the alternating group, a desirable property. Further work on this theme

* This work was supported by The Royal Society through its European Science Exchange Programme and the Swiss National Science Foundation, and was performed whilst the author was visiting ETH Zurich.

can be found in [22]. In [26] it was shown that the actual round functions of the DES generate the alternating group. The question of whether the $2^{56}$ encryptions of the full DES themselves form a group, or generate a small group (see [12, 20]), was answered in the negative in [5] and a lower bound of $10^{2499}$ was obtained in [4] for the size of this generated group. Thus the attacks of [12] are not applicable to the DES.

In [11], the groups generated by the round function of "mini-versions" of the block cipher IDEA [17] were calculated.

However the ability of a cipher (or its round functions) to generate a large group does not alone guarantee security: an example of a weak cipher generating the symmetric group on the message space was given recently in [21]. The most that can be said is that a small group may lead to an insecurity.

Here we examine properties of the groups related to a block cipher more refined than simply their size. Consider the following statement of Wernsdorf [26] regarding the group generated by the round functions of DES:

> "Since the generated alternating group $A_{2^{64}}$ is a large simple group and primitive on $V_{64}$ [the message space] we can exclude several imaginable cryptanalytic 'shortcuts' of the DES algorithm."

In the next section we will formalise our discussion of the groups associated with iterated block ciphers and sketch the theory of primitive and imprimitive groups. Next, motivated by Wernsdorf's statement, we examine attacks on iterated block ciphers whose round functions generate imprimitive groups. Then we argue that these imprimitivity-based attacks enable a designer to build trapdoors into iterated block ciphers. We give an example of a 64-bit DES-like cipher having 32 rounds and an 80-bit key which is resistant to linear and differential cryptanalysis but whose security is severely compromised by such an attack using $2^{32}$ chosen plaintexts. With a careful (and deliberately weak) choice of key-schedule and knowledge of the trapdoor, the cipher can be completely broken using only a few known plaintexts and $2^{41}$ trial encryptions. While the trapdoor in our example is not so well disguised, it can easily be made undetectable if the cipher design is not made public. We conclude by giving some implications of our work and ideas for future research.

We mention here the recent work of [24] in which block ciphers containing *partial* trapdoors are constructed: these give only partial information about keys and require rather large S-box components to be present in the cipher. However, they are computationally undetectable. In contrast, our trapdoor can be inserted into a block cipher with very small

S-boxes, reveals the entire key, but is detectable. In the language of [24], it is a full, but detectable, trapdoor. It is a moot point whether full and undetectable trapdoors can be inserted in truly practical block ciphers.

## 2 Iterated Block Ciphers and their Groups

We begin by describing a model for *iterated block ciphers*. We will regard such a cipher as a set of invertible *encryption functions* mapping a set $M$, the message space, to itself, or equivalently as a subset of the symmetric group on $M$, denoted $S_M$. We can then use notions from the theory of permutation groups to study such ciphers. The necessary algebraic background can be found in [25] or [27].

The encryption functions of a particular iterated block cipher are obtained by the composition of *round functions*, that is, a set of keyed invertible functions on $M$, which we denote by $\{R_k : M \to M,\ k \in K\}$. Here $K$ is called the *round keyspace* and $k$ a *round key*. In a $t$-round iterated block cipher, the encryption functions take the form

$$E_{k_1,\ldots,k_t} = R_{k_1} R_{k_2} \cdots R_{k_t}$$

where the $k_i$ may be derived from a key from a (larger) session keyspace according to some key-scheduling algorithm, or may be independently chosen. Thus, the encryption of plaintext $m$ under round keys $k_1, k_2, \ldots, k_t$ is

$$mE_{k_1,\ldots,k_t} = mR_{k_1} R_{k_2} \cdots R_{k_t}$$

(for the moment we denote all functions as acting on the right of their arguments, so that in a composition, functions are evaluated from left to right).

We write $G =< R_k : k \in K >$ for the group generated by the round functions, that is, the smallest subgroup of $S_M$ containing each $R_k$. Similarly we write $G_t =< R_{k_1} \ldots R_{k_t} : k_i \in K >$ for the subgroup of $S_M$ generated by the $t$-round encryptions with independent round keys. We say that $G$ and the $G_t$ *act* on the message space $M$. The groups $G_t$ are hard to compute in practice, but we have the following result relating them to the group $G$ generated by the round functions:

**Theorem 1 ([11]).** *With notation as above, $G_t$ is a normal subgroup of $G$. Moreover the group generated by the $t$-round encryptions with round keys from a particular key-schedule is a subgroup of $G_t$.*

*Example 1.* The DES (described in full in [7]) is essentially an iterated block cipher with $t = 16$ rounds, message space $M = V_{64}$, the vector-space of dimension 64 over $\mathbf{Z}_2$, and round keyspace $K = V_{48}$. The form taken by the round functions $R_k$ of the DES is:

$$mR_k = (l, r)R_k = (r, l \oplus f(r, k))$$

where $l, r \in V_{32}$ denote the left and right halves of message $m$ and $f : V_{32} \times V_{48} \to V_{32}$. The group $G$ generated by the round functions of the DES is known to be the alternating group on $V_{64}$, denoted $A_{2^{64}}$, [26]. Since $G$ is simple and $G_{16}$ is normal in $G$, the group generated by the DES with independent round keys is also $A_{2^{64}}$. The group generated by the DES itself (with key-schedule as defined in [7]) is not known.

We will follow the exposition of [27], Sections 6 and 7 on imprimitive groups. Our presentation is necessarily compressed.

Let $G$ be a group of permutations acting on a set $M$ (the reader can imagine $G$ and $M$ to be as above). A subset $Y$ of $M$ is said to be a *block* of $G$ if for each $g \in G$,

$$\text{either} \quad Yg = Y \quad \text{or} \quad Yg \cap Y = \emptyset.$$

Here $Yg$ denotes the set $\{yg : y \in Y\}$. The sets $M$, $\emptyset$ and the singletons $\{y\}$ are blocks of every $G$ acting on $M$. These are called the trivial blocks. The intersection of two blocks of $G$ is also a block.

If $Y$ is a block of $G$, then so is $Yg$ for every $g \in G$. The set of distinct blocks obtained from a block $Y$ in this way is called a *complete block system*. All blocks of such a system have the same size and if $G$ is transitive on $M$, then every element of $M$ lies in a block of the system. Thus, in this case, the blocks form a partition of $M$ into disjoint sets of equal size.

Suppose now that $G$ is transitive. Then $G$ is said to be *imprimitive* (or act *imprimitively*) if there is at least one non-trivial block $Y$. We will then refer to a *complete non-trivial block system*. Otherwise, $G$ is said to be *primitive*.

Let $G$ act imprimitively on a finite set $M$ and let $Y$ be a block of $G$, with $|Y| = s$. Since $G$ is transitive, there exist elements $1 = \tau_1, \tau_2, \ldots, \tau_r \in G$ such that the sets

$$Y_1 = Y\tau_1 = Y, Y_2 = Y\tau_2, \ldots, Y_r = Y\tau_r$$

form a complete non-trivial block system. Here, $|M| = rs$. Thus, for every $g \in G$, there exists a permutation $\overline{g}$ of $\{1, 2, \ldots, r\}$ such that

$$Y_i g = Y_{i\overline{g}}.$$

The set of $\overline{g}$ form a permutation group $\overline{G}$ on $\{1, 2, \ldots, r\}$ and the map $g \to \overline{g}$ is a group homomorphism from $G$ onto $\overline{G}$.

## 3 Attacks Based on Imprimitivity

Suppose the group $G$ generated by the round functions $R_k : M \to M$ of a $t$-round cipher acts imprimitively on $M$, and let $Y_1, \ldots, Y_r$ be a complete non-trivial block system for $G$. Suppose further that, given $m \in M$, there is a description of the blocks such that it is easy to compute the $i$ with $m \in Y_i$ and that round keys $k_1, \ldots, k_t$ are in use.

Our basic attack is a chosen-plaintext attack whose success is independent of the number $t$ of rounds in use.

### 3.1 Basic Attack

Suppose that we choose one plaintext $m_i$ in each set $Y_i$ and obtain the corresponding ciphertext $c_i$. Then the effect of $g = R_{k_1} R_{k_2} \ldots R_{k_t}$ on the blocks $Y_i$ is determined. For by the imprimitivity of $G$,

$$c_i = m_i g \in Y_j \quad \Rightarrow \quad Y_i g = Y_j.$$

Now given any further ciphertext $c$, we compute $l$ such that $c \in Y_l$. Then the plaintext $m$ corresponding to $c$ satisfies $m \in Y_{l\overline{g}^{-1}}$. Thus $r$ chosen plaintexts determine that the message corresponding to any ciphertext must lie in a set of size $\frac{|M|}{r}$. Hence the security of the system is severely compromised. The plaintext $m$ itself can be found by examining the set of meaningful messages in $Y_{k\overline{g}^{-1}}$.

Alternatively, the basic attack determines the permutation $\overline{g}$ of $\overline{G}$ corresponding to $g$: we can think of $\{1, \ldots, r\}$ as being the message space of a new cipher (where the encryption of $i$ is $i\overline{g}$ for round keys $k_1, \ldots, k_t$) and regard our basic attack as simply obtaining all the plaintext/ciphertext pairs for a fixed set of round keys.

### 3.2 Key-Schedule Dependent Attack

Every choice of round keys $k_1, \ldots, k_t$ determines a corresponding permutation $\overline{g}$ of $\{1, 2, \ldots, r\}$. It is conceivable that there is an attack on the new cipher more efficient than exhaustively obtaining all the ciphertexts. Ideally such an attack would also obtain key information. As an important example, the round keys may be derived from a session key in such a way that $\overline{g}$ is wholely determined by only a part of the session key information.

In practice, this information might take the form of the values of certain bits of the session key, or the value of linear expressions involving session key bits. We can think of $\overline{g}$ as being determined by keys from a reduced keyspace. Then it may be feasible to carry out an exhaustive search of the reduced keyspace using only a few known plaintext/ciphertext pairs to determine a unique reduced key. Given such session key information, it may then be possible to deduce the complete session key by another exhaustive search. We have a divide-and-conquer attack on the session key.

This latter attack is then closely related to the attacks of [23] and [9] on ciphers whose round functions possess linear factors and linear structures respectively. For example, when $M = V_n$ and the $Y_i$ consist of a linear subspace $U$ of $V_n$ and its cosets, we have a special type of linear factor (as described in [23]) where the plaintext and ciphertext maps are equal and map coset $Y_i = U + a_i$ to $a_i$.

### 3.3 Multiple Block System Attack

In an extension of the basic attack, we make use of two or more complete non-trivial block systems.

*Example 2.* Using the notation of example 1, we define an $f$ function as follows: we divide the input $r$ to the $f$ function into two halves $r_1, r_2 \in V_{16}$ and define

$$f(r,k) = (f_1(r_1,k), f_2(r_2,k))$$

where $f_i : V_{16} \times K \to V_{16}$ are arbitrary. It was shown in [16] that the $f_i$ can be chosen so that the iterated block cipher with round function $(l,r)R_k = (r, l \oplus f(r,k))$ is secure against linear and differential cryptanalysis. We model an attack based on two complete systems of imprimitivity: we write elements of $V_{64}$ as $(x_1,x_2,x_3,x_4)$ where $x_i \in V_{16}$ and define $2^{33}$ sets of size $2^{32}$:

$$\begin{aligned} Y_{(x_1,x_3)} &= (x_1, V_{16}, x_3, V_{16}), \\ Z_{(x_2,x_4)} &= (V_{16}, x_2, V_{16}, x_4). \end{aligned}$$

Notice that

$$\begin{aligned} Y_{(x_1,x_3)}R_k &= (x_3, V_{16}, x_1 \oplus f_1(x_3,k), V_{16}) = Y_{(x_3, x_1 \oplus f_1(x_3,k))} \\ Z_{(x_2,x_4)}R_k &= (V_{16}, x_4, V_{16}, x_2 \oplus f_2(x_4,k)) = Z_{(x_4, x_2 \oplus f_2(x_4,k))} \end{aligned}$$

so that the sets $\left\{Y_{(x_1,x_3)} : x_1, x_3 \in V_{16}\right\}$ and $\left\{Z_{(x_2,x_4)} : x_2, x_4 \in V_{16}\right\}$ form complete block systems for $G$, the group generated by the $R_k$. Moreover, for any $x_1, x_2, x_3, x_4$,

$$Y_{(x_1,x_3)} \cap Z_{(x_2,x_4)} = \{(x_1, x_2, x_3, x_4)\}.$$

Suppose we choose the $2^{32}$ plaintexts of the form $(x_1, x_1, x_3, x_3)$ and obtain their encryptions. From this information we can recover permutations $\overline{g}_1$ and $\overline{g}_2$ of $V_{16} \times V_{16}$ such that for all $x_1, x_2, x_3, x_4$

$$Y_{(x_1,x_3)}g = Y_{(x_1,x_3)\overline{g}_1}, \qquad Z_{(x_2,x_4)}g = Z_{(x_2,x_4)\overline{g}_2}.$$

Given any further ciphertext $(c_1, c_2, c_3, c_4)$ with corresponding message $m$ we have

$$m \in Y_{(c_1,c_3)\overline{g}_1^{-1}} \cap Z_{(c_2,c_4)\overline{g}_2^{-1}},$$

a set of size one. Thus $m$ can be found uniquely.

This attack is applicable to any cipher where the intersections of blocks from different systems can be computed and are "small".

## 4 A DES-like Cipher with a Trapdoor

Given the description of a set of round functions, it appears to be a difficult computational problem either to find a non-trivial complete block system for the corresponding group $G$ or to disprove the existence of such a system. However the attacks above show that an iterated block cipher with an imprimitive group $G$ is inherently weak if a complete block system is known.

It appears then that using a set of round functions which generate an imprimitive group (whose block system is not revealed) may lead to a block cipher containing a trapdoor that is difficult to detect. To give a convincing demonstration of this, we should build a set of round functions according to recognised principles (e.g. Shannon's principles of diffusion and confusion). The individual components should satisfy relevant design criteria and we should also demonstrate the security of our cipher against known attacks. This is our objective in this section. We give a full design for such a block cipher, except for a key-schedule. In the next section we will describe how our round functions were designed to generate an imprimitive group and how the cipher can be broken.

### 4.1 Description of Round Function

Perhaps the most commonly used template in the design of a block cipher is the Feistel construction. In turn the most celebrated Feistel-type cipher is the DES itself. With reference to example 1 and [7], the $f$ function of the DES consists of four components: we write $f(r,k) = PS(E(r) \oplus k)$ where

— the expansion phase, $E$, is a linear map from $V_{32}$ to $V_{48}$,
— $k$ is the 48-bit round key, derived from a 56 bit session key,
— $S$ denotes the operation of the S-boxes — eight carefully selected 6 bit to 4 bit functions, numbered $1, \ldots, 8$ operating in parallel on $V_{48}$,
— $P$ is a carefully selected bit permutation of $V_{32}$.

Our proposed block cipher consists of 32 repetitions of DES-like round functions:

$$(l,r)R_k = (r, l \oplus PS(E(r) \oplus k)).$$

Here $E$ and $P$ are as in the original DES, but the S-boxes are replaced by the boxes presented in the appendix. Our round keys $k$ are also 48-bits and are derived from an 80-bit session key according to a key-scheduling algorithm which we leave unspecified. Any suitably strong schedule could be used (for example, we could expand the original DES schedule).

We note that the selection of S-boxes is critical to the security of the DES. Numerous attacks have been made on versions of the DES with modified S-boxes: see for example the early critique of DES in [10], the differential attacks on the DES with modified S-boxes in [2] and the attack of [15] on the proposals of [13].

Each S-box in the appendix has the following properties, similar to those given in [5] for the DES S-boxes:

S1 Each S-box has six bits of input, four bits of output.
S2 The best linear approximation of an S-box (in the sense of [18], equation (3)) holds with probability $p$ over all inputs, where $|p - \frac{1}{2}| \leq \frac{1}{4}$.
S3 Fixing the bits input to an S-box on the extreme left and on the extreme right at any two values, the resulting map from $V_4$ to $V_4$ is a permutation.
S4 If two inputs $i, i'$ to an S-box differ in the pattern 000100 or 001000 (i.e. $i \oplus i' = 000100$ or 001000), then the corresponding outputs differ in at least one position.
S5 If two inputs $i, i'$ to an S-box differ in the pattern 001100, then the corresponding outputs differ in at least one position.

S6 If two inputs $i, i'$ satisfy $i \oplus i' = 11xy00$, where $x$ and $y$ are arbitrary bits, then the corresponding outputs differ in at least one position.

S7 For any non-zero input difference $i \oplus i'$ not equal to one of those specified in S4, S5, the number of ordered pairs $i, i'$ leading to a given non-zero output difference is at most 16. For the input differences in S4 and S5, the corresponding maximum is 24.

S8 For any non-zero input difference $i \oplus i'$, the number of ordered pairs $i, i'$ leading to an output difference of zero is at most 12.

S2 guarantees that the S-boxes are not too linear, while S3 ensures they are balanced. S4–S6 can be regarded as weak avalanche criteria. Thus our S-boxes automatically have some desirable features.

We also draw to the reader's attention the properties P1 to P3 of the $P$ permutation noted in [5]. From left to right, we label the input bits to our S-boxes $p_1, p_2, p_3, p_4, p_5, p_6$ and the output bits $q_1, q_2, q_3, q_4$. We refer to bits $p_3$ and $p_4$ as *centre* bits and bits $p_1, p_2, p_5, p_6$ as *outer* bits.

P1 The four bits output from each S-box are distributed so that two of them affect centre bits, and the other two affect outer bits of S-boxes in the next round.

P2 The four bits output from each S-box affect six different S-boxes in the next round, no two affect the same S-box.

P3 For two S-boxes $j$, $k$, if an output bit from S-box $j$ affects a centre bit of S-box $k$, then an output bit from S-box $k$ cannot affect a centre bit of S-box $j$.

### 4.2 Security Against Linear and Differential Attacks

Here we estimate the resistance of our example to linear [18] and differential [2, 3] cryptanalysis.

We begin by estimating the complexity of a linear attack. By property S2 and Lemma 3 of [18], the best linear expression that is built up round-by-round and involves input bits to round 2, output bits from round 31, key bits and a linear approximation in *every* round will hold with approximate probability $p_L$ where

$$|p_L - \frac{1}{2}| \leq 2^{29} \left(\frac{1}{4}\right)^{30} = 2^{-31}.$$

While a more delicate analysis may find linear characteristics not involving linear approximations in every round, it seems unlikely that these will have probability larger than the above bound on $p_L$ (since this bound is

calculated using the highest per-round probability). We make the rough assumption that a linear attack using Algorithm 2 of [18] would require at least $2^{62}$ known plaintexts.

The success of a differential attack depends on finding a high probability characteristic: a *t-round characteristic having probability p* is a sequence of differences

$$\Delta m_1, \Delta m_2, \ldots, \Delta m_{t-1}, \Delta m_t$$

such that if $\Delta m_1$ is the difference in plaintexts $m \oplus m'$ input to the first round, then the differences propagated to the inputs of subsequent rounds are $\Delta m_2, \ldots \Delta m_t$ with probability $p$, assuming independent round keys. In practice, at least a 29 round characteristic is needed to attack a 32 round iterated cipher. The number of plaintext input pairs required in a successful attack based on such a characteristic having probability $p$ is at least $\frac{1}{p}$. Of particular importance are *iterative characteristics* where the output difference at the last round is equal to the initial input difference — such a characteristic can be concatenated with itself many times to form a longer characteristic. To provide practical security against a differential attack, we need to bound the probability of short iterative characteristics. For further details, see [2, 3].

We say that an S-box $j$ is *active* in round $i$ of a characteristic if $\Delta m_i$ involves a non-zero input difference to S-box $j$. We can use properties S3 to S6, P2 and P3 and arguments similar to those of [5] to show the following for our cipher:

**Lemma 1.** *If round $i$ of a characteristic consists of two adjacent active S-boxes $j, j+1$ then either round $i-1$ or round $i+1$ (or both) has at least one active S-box. If round $i$ of a characteristic has only one active S-box $j$, then either round $i-1$ or round $i+1$ (or both) has at least one active S-box.*

A 29 round characteristic having no rounds without active S-boxes must involve a total of at least 29 active S-boxes. Using S7 and assuming independence, we can bound the probability of such a pattern by $p \leq \left(\frac{24}{64}\right)^{29} = 2^{-41}$. We have found characteristics with probability close to this, but omit the details. An attractive pattern of differences (used in [3] to attack the DES) involves active S-boxes on even numbered rounds and no active S-boxes on odd numbered rounds. From the above lemma, the active rounds must involve at least a pattern of 3 adjacent S-boxes. By property S8, we can bound the probability of a 29 round pattern of

this type by $\left(\frac{12}{64}\right)^{42} = 2^{-101}$. One further pattern of differences that we consider involves no active S-boxes on every third round. Using P3 and the lemma above, we can show that such a characteristic must involve 3 or more active S-boxes on the two active rounds. The probability of such a characteristic over 29 rounds is, using S7, at most $2^{-41}$. The analysis can be carried further, but it suffices to note here that our cipher possesses a reasonable degree of resistance to differential cryptanalysis.

## 5 Trapdoor Design

Each S-box in the appendix has the following property:

> By property P1, the combination of $P$ followed by $E$ moves two of the four outputs of the S-box (say $q_i$ and $q_j$) so as to affect centre bits of S-boxes in the next round. These two outputs are dependent on every input bit, while the other two outputs depend only on the outer bits $p_1, p_2, p_5, p_6$ input to the S-box.

For example, $P$ moves output bit $q_3$ of S-box 1 to position 23 in the output of the $f$ function. After XORing with the left half and swopping, this position affects a centre bit, $p_4$, of S-box 6 in the next round. Thus $q_3$ depends on all six input bits to S-box 1.

From the property above, it follows that the output bits of the $f$ function in positions $1, 4, 5, 8, \ldots, 29, 32$ depend only on round key bits and the $f$ function inputs in the same positions, $1, 4, 5, 8, \ldots, 29, 32$ (these being the $f$ function input bits which after $E$ and key XOR become outer bits of S-boxes). We therefore have:

**Lemma 2.** *Label the* $2^{16}$ *distinct additive cosets of the* 16 *dimensional subspace*

$$U = \{(0, x_2, x_3, 0, 0, x_6, x_7, 0, \ldots, 0, x_{30}, x_{31}, 0) : x_i \in \mathbf{Z}_2\}$$

*of* $V_{32}$ *by* $U \oplus a_1, \ldots, U \oplus a_{2^{16}}$. *Then for every* $j$ *and every round key* $k$, *there exists an* $l$ *such that* $PS(E(U \oplus a_j) \oplus k) \subseteq U \oplus a_l$.

Notice that for any subset $W$ of subspace $U$, we have $U \oplus W = U$, so

$$(U \oplus a_i) \oplus PS(E(U \oplus a_j) \oplus k)) = U \oplus a_i \oplus a_l = U \oplus a_m$$

for some $m$. Therefore $(U \oplus a_i, U \oplus a_j)R_k = (U \oplus a_j, U \oplus a_m)$. It is easy to see that the $R_k$ act transitively on $V_{64}$ and we have

**Lemma 3.** *The $2^{32}$ subsets $(U \oplus a_i, U \oplus a_j)$ of $V_{64}$ form a complete non-trivial block system for $G$, the group generated by the round functions of our cipher.*

The round functions of our cipher generate an imprimitive group where the blocks of a complete system are easily identified. Thus our cipher is susceptible to the basic attack described in Section 3 with $2^{32}$ chosen plaintexts. Suppose further that a key-schedule is chosen such that over the 32 rounds, only 40 bits of the 80-bit session key are involved in XORs with outputs of the $E$ expansion which become outer bits of the S-boxes. Then, in the terminology of Section 3, the permutation $\overline{g}$ is determined by only half of the session key bits and an exhaustive attack on those bits can be successfully carried out with knowledge of a handful of plaintext/ciphertext pairs. The remaining 40 bits of session key can then also be found by exhaustive attack, the total complexity of the attack being around $2^{41}$ trial encryptions, well within the bounds of practicality. Notice that this attack depends crucially on the interaction between the system of imprimitivity and the key-schedule.

## 6 Discussion and Conclusions

We have considered attacks based on a property of a group associated with an iterated block cipher. The attacks motivate a new design criterion for iterated block ciphers: the group generated by the round functions should be primitive. Unfortunately this property seems to be hard to verify in practice. We note that the DES and (probably) IDEA do satisfy this property.

We have given an example of a cipher secure in many conventional senses but weak because of a deliberately inserted trapdoor. There are however some immediate criticisms that can be made of our example. Firstly, the S-boxes are incomplete (that is, not every output bit of the S-boxes depends on every input bit). This goes against a generally accepted design principle for S-boxes [1, 14, 19] and would arouse suspicion. A close examination of the S-boxes and their interaction with the $P$ permutation would then reveal our trapdoor. Incompleteness in the S-boxes also leads to a block cipher where half of the ciphertext bits are independent of half of the plaintext bits. Thus our trapdoor is not so well hidden. Secondly and less seriously, our cipher's resistance to differential attacks is not as high as one might expect from a 32 round system.

Suppose however that the round function design and weak key-schedule algorithm of our example are not made public (for example, by using

tamper-resistant hardware). We are then given a 64-bit iterated block cipher with 32 rounds and an 80-bit key and could be truthfully told by a panel of experts that it is secure against linear and differential attacks. The incompleteness noted above can be hidden by applying a suitable invertible output transformation to the ciphertexts. Because of the size of the message space and choice of output transformation, we would then be unlikely to be able to detect any block structure just by examining plaintext/ciphertext pairs. Yet our example cipher contains a trapdoor rendering the system completely insecure to anyone with knowledge of the trapdoor. Clearly in this situation, we must have complete faith in the purveyor of the block cipher.

We conclude by suggesting some avenues for further research.

The choice of trapdoor in our example was forced upon us by a combination of the $E$ expansion, the round key XORing and the bitwise nature of the $P$ permutation. Can "undetectable" trapdoors based on more complex systems of imprimitivity be inserted in otherwise conventional ciphers? It is easily shown that, in a DES-like cipher, any system based on a linear sub-space and its cosets leads to a noticeable regularity in the XOR tables of small S-boxes. It seems that we must look beyond the "linear" systems considered here, or consider other types of round function.

Our attention has been directed to block systems preserved by the group $G$, that is, on a per-round basis. It might also be interesting to look at the case where the round functions generate a primitive group, but the subgroup generated by the $t$-round cipher itself has a block structure. Attacks exploiting a block structure holding probablistically may also be powerful and worth examining.

## Acknowledgements

The author would like to thank Jim Massey for his encouragement during this research, and Lars Knudsen for patiently answering my many questions and for his humour. Carlo Harpes also made useful comments on an early version of this paper.

### References

1. C.M. Adams and S.E. Tavares, "The Structured Design of Cryptographically Good S-boxes." Journal of Cryptology **3** (1990) 27–41.

2. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems." Journal of Cryptology **4** (1991) 3–72.
3. E. Biham and A. Shamir, "Differential Cryptanalysis of the Full 16-round DES." Proceedings of CRYPTO'92 LNCS 740 (1993) 487–496.
4. K.W. Campbell and M. Wiener, "DES is not a Group." Proceedings of CRYPTO'92 LNCS 740 (1993) 512–520.
5. D. Coppersmith, "The Data Encryption Standard (DES) and its Strength Against Attacks." IBM Research Report, RC 18613 (1992).
6. D. Coppersmith and E. Grossman, "Generators for Certain Alternating Groups with Applications to Cryptology." SIAM Journal on Applied Mathematics **29** (1975) 624–627.
7. "Data Encryption Standard." National Bureau of Standards, Federal Information Processing Standards Publications No. 46 (1977).
8. S. Even and O. Goldreich, "DES-like Functions Can Generate the Alternating Group." IEEE Transactions on Information Theory **29** (1983) 863–865.
9. J.-H. Evertse, "Linear Structures in Blockciphers." Proceedings EUROCRYPT'87 LNCS 304 (1988) 249–266.
10. M. Hellman, R. Merkle, R. Schroeppel, L. Washington, W. Diffie, S. Pohlig and P. Schweitzer, "Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption Standard." Information Systems Laboratory report, Stanford University (1976).
11. G. Hornauer, W. Stephan and R. Wernsdorf, "Markov Ciphers and Alternating Groups." Presented at Rump Session, EUROCRYPT'93 (1993).
12. B.S. Kaliski Jr., R.L. Rivest and A.T. Sherman, "Is the Data Encryption Standard a Group? (Results of Cycling Experiments on DES)." Journal of Cryptology **1** (1988) 3–36.
13. K. Kim, "Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC." Proceedings of ASIACRYPT'91 LNCS 739 (1992) 59–72.
14. B. Kam and G.I. Davida, "A Structured Design of Substitution-Permutation Encryption Networks." IEEE Transactions on Computers **28** (1979) 747–753.
15. L.R. Knudsen, "Iterative Characteristics of DES and $s^2$-DES." Proceedings of CRYPTO'92 LNCS 740 (1993) 497–511.
16. L. R. Knudsen, "Practically Secure Feistel Ciphers." Fast Software Encryption LNCS 809 (1994) 211-221.
17. X. Lai, J.L. Massey and S. Murphy, "Markov Ciphers and Differential Cryptanalysis". Proceedings of EUROCRYPT'91 LNCS 547 (1991) 17–38.
18. M. Matsui, "Linear Cryptanalysis Method for DES Cipher." Proceedings of EUROCRYPT'93 LNCS 765 (1994) 386–397.
19. W. Meier and O. Staffelbach, "Nonlinearity Criteria for Cryptographic Functions." Proceedings of EUROCRYPT'89 LNCS 434 (1989) 549–562.
20. J.H. Moore and G.J. Simmons, "Cycle Structure of the DES with Weak and Semiweak Keys." Proceedings of CRYPTO'86 LNCS 263 (1987) 9–32.
21. S. Murphy, K. Paterson and P. Wild, "A Weak Cipher that Generates the Symmetric Group." Journal of Cryptology **7** (1994) 61–65.
22. J. Pieprzyk and X.-M. Zhang, "Permutation Generators of Alternating Groups." Proceedings of AUSCRYPT'90 LNCS 453 (1990) 237–244.
23. J.A. Reeds and J.L. Manferdelli, "DES Has No Per Round Linear Factors." Proceedings of CRYPTO'84 LNCS 196 (1985) 377–389 .
24. V. Rijmen and B. Preneel, "A family of trapdoor ciphers," Fast Software Encryption LNCS 1267 (1997) 139–148.

25. D.J.S. Robinson, "A Course in the Theory of Groups". Graduate Texts in Mathematics, Springer, New York (1982).
26. R. Wernsdorf, "The One-Round Functions of the DES Generate the Alternating Group." Proceedings of EUROCRYPT'92 LNCS 658 (1993) 99–112.
27. H. Wielandt, "Finite Permutation Groups." Academic press, New York and London (1964).

## Appendix

We present the S-boxes of our example block cipher in the same format as the DES S-boxes were presented in [7], that is each box is written as four rows of permutations:

S-box 1

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | 0 | 10 | 1 | 9 | 3 | 11 | 2 | 4 | 12 | 7 | 14 | 6 | 15 | 5 | 13 |
| 9 | 5 | 10 | 7 | 8 | 4 | 11 | 6 | 14 | 1 | 13 | 0 | 12 | 2 | 15 | 3 |
| 14 | 10 | 15 | 11 | 12 | 9 | 13 | 8 | 1 | 5 | 2 | 7 | 0 | 4 | 3 | 6 |
| 11 | 5 | 9 | 4 | 8 | 6 | 10 | 7 | 1 | 14 | 0 | 12 | 3 | 15 | 2 | 13 |

S-box 2

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 15 | 0 | 12 | 3 | 13 | 2 | 14 | 6 | 9 | 5 | 8 | 4 | 10 | 7 | 11 |
| 11 | 1 | 10 | 2 | 8 | 0 | 9 | 3 | 6 | 15 | 7 | 13 | 5 | 12 | 4 | 14 |
| 1 | 14 | 3 | 12 | 0 | 15 | 2 | 13 | 8 | 6 | 10 | 4 | 9 | 5 | 11 | 7 |
| 2 | 5 | 1 | 7 | 0 | 6 | 3 | 4 | 15 | 8 | 14 | 9 | 13 | 10 | 12 | 11 |

S-box 3

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 11 | 13 | 9 | 12 | 10 | 14 | 8 | 3 | 4 | 1 | 6 | 0 | 7 | 2 | 5 |
| 0 | 14 | 1 | 12 | 2 | 15 | 3 | 13 | 10 | 6 | 8 | 5 | 11 | 7 | 9 | 4 |
| 14 | 1 | 13 | 2 | 15 | 0 | 12 | 3 | 8 | 7 | 11 | 6 | 10 | 5 | 9 | 4 |
| 4 | 12 | 7 | 13 | 6 | 14 | 5 | 15 | 11 | 3 | 8 | 2 | 9 | 0 | 10 | 1 |

S-box 4

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 | 3 | 6 | 1 | 4 | 11 | 14 | 9 | 7 | 2 | 15 | 10 | 5 | 0 | 13 | 8 |
| 5 | 3 | 15 | 11 | 7 | 9 | 13 | 1 | 6 | 10 | 14 | 8 | 12 | 0 | 4 | 2 |
| 4 | 9 | 14 | 11 | 12 | 1 | 6 | 3 | 2 | 7 | 0 | 15 | 10 | 13 | 8 | 5 |
| 15 | 4 | 5 | 12 | 13 | 14 | 7 | 6 | 9 | 10 | 11 | 8 | 1 | 0 | 3 | 2 |

S-box 5

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 6 | 4 | 7 | 0 | 2 | 5 | 3 | 13 | 10 | 8 | 14 | 9 | 15 | 12 | 11 |
| 2 | 4 | 7 | 0 | 6 | 5 | 3 | 1 | 9 | 14 | 13 | 15 | 8 | 10 | 12 | 11 |
| 0 | 13 | 4 | 9 | 1 | 12 | 5 | 8 | 7 | 15 | 6 | 10 | 2 | 11 | 3 | 14 |
| 11 | 2 | 15 | 7 | 14 | 3 | 10 | 6 | 1 | 13 | 4 | 12 | 5 | 8 | 0 | 9 |

S-box 6

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | 5 | 11 | 4 | 9 | 6 | 10 | 7 | 1 | 14 | 3 | 15 | 2 | 13 | 0 | 12 |
| 7 | 3 | 6 | 0 | 4 | 1 | 5 | 2 | 9 | 14 | 11 | 13 | 8 | 12 | 10 | 15 |
| 7 | 8 | 6 | 10 | 5 | 9 | 4 | 11 | 3 | 15 | 0 | 14 | 2 | 12 | 1 | 13 |
| 12 | 6 | 15 | 7 | 14 | 4 | 13 | 5 | 2 | 11 | 1 | 9 | 0 | 8 | 3 | 10 |

S-box 7

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 | 3 | 15 | 1 | 14 | 2 | 13 | 0 | 11 | 5 | 10 | 7 | 8 | 6 | 9 | 4 |
| 12 | 6 | 13 | 5 | 14 | 4 | 15 | 7 | 0 | 9 | 3 | 10 | 1 | 8 | 2 | 11 |
| 1 | 12 | 3 | 14 | 2 | 13 | 0 | 15 | 9 | 7 | 8 | 4 | 11 | 6 | 10 | 5 |
| 11 | 14 | 9 | 15 | 8 | 13 | 10 | 12 | 4 | 1 | 7 | 3 | 5 | 2 | 6 | 0 |

S-box 8

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 | 5 | 10 | 7 | 8 | 3 | 14 | 1 | 6 | 11 | 0 | 9 | 4 | 15 | 2 | 13 |
| 11 | 12 | 13 | 8 | 9 | 10 | 15 | 14 | 2 | 3 | 0 | 1 | 6 | 5 | 4 | 7 |
| 3 | 8 | 7 | 12 | 5 | 10 | 1 | 14 | 0 | 13 | 6 | 15 | 2 | 9 | 4 | 11 |
| 5 | 13 | 3 | 9 | 1 | 11 | 7 | 15 | 10 | 0 | 8 | 6 | 12 | 4 | 14 | 2 |