DES-LIKE FUNCTIONS CAN
GENERATE THE ALTERNATING GROUP

by

S. Even and O. Goldreich

Technical Report #258
(This is a revised version of Report #207)
January 1983

* The research was supported by the Fund for the Promotion of Research at the Technion.
ABSTRACT

A set of transformations on binary vectors of length n is defined. These transformations are similar to those of the DES and therefore are called DES-like-functions. It is proved that the group of permutations generated by the DES-like-functions is exactly the Alternating Group of the set of binary n-vectors.
1. INTRODUCTION

In the design of block ciphers, it is considered a virtue if the encipherment can perform all the \( (2^n)! \) permutations on \( n \)-vectors, where \( n \) is large enough to prevent the feasibility of applying the usual techniques for cryptanalyzing a substitution code. However, this is an impractical target since such a system would require a key of length \( \log_2(2^n)! \approx n \cdot 2^n \). Thus, one is inclined to weaken the requirement and seek a cryptosystem in which one can perform every permutation by repeated encipherments.

Coppersmith and Grossman [1] defined \( k \)-functions and explored the group of all permutations generated by them. It was mentioned that such functions are similar to some block-ciphers and thus the use of such to cryptography should be studied.

The DES is a well-known and used [2] block cipher. We define DES-like-functions which operate on restricted fixed blocks and are similar to the structure used in the DES. We show that such functions can generate the Alternating Group and thus satisfy the weak requirement mentioned above. This is by no means a proof of their cryptographic power. However, had the group generated by these functions been "small" an inherent weakness of the cipher based on them would have been established.

2. DEFINITIONS

(1) \( \mathbb{V}_n \) is the vector space of dimension \( n \) over \( \mathbb{GF}(2) \).

* Ciphers in which the messages and the cryptograms are binary vectors of a fixed length \( n \) are called block ciphers.
(2) \( S_X \) is the group of all permutations on a set \( X \), and is called the Symmetric Group of \( X \).

(3) \( A_X \) is the group of all even permutations on a set \( X \), called the Alternating Group of \( X \). A permutation is called even iff it can be expressed by an even number of transpositions (i.e. cycles of length two).

(4) Let \( 1 \leq k \leq n \). Define a \( k \)-function on \( V_n \) to be a transformation \( \sigma \) on \( V_n \) determined by the subset \( \{ i \} \subseteq \{ i \} \) and a function \( f: V_k \rightarrow V_1 \) as follows:

\[
(a_1, \ldots, a_i, \ldots, a_n) \sigma = (a_1, \ldots, a_i^{k+1}, \ldots, a_n),
\]

where the symbol \( \oplus \) denotes addition modulo 2.

Notice that for any \( k \)-function \( \sigma \), \( \sigma^2 \) = identity, proving that \( \sigma \) is a permutation on \( V_n \).

We denote by \( G_{k,n} \) the subgroup of \( S_{V_n} \) generated by \( k \)-functions.

(5) By a DES-like-function on \( V_{2n} \) we mean a transformation \( \delta_f \) on \( V_{2n} \) determined by a function \( f: V_n \rightarrow V_n \) as follows:

\[
(\hat{x}, \hat{y}) \delta_f = (\hat{y}, \hat{x} \oplus f(\hat{y})) \quad \text{where} \quad \hat{x}, \hat{y} \in V_n \quad \text{and} \quad \text{the symbol} \quad \oplus \quad \text{denotes the bit by bit addition modulo 2.}
\]

Notice that we can write \( \delta_f = \sigma_f \cdot \theta \) where \( (\hat{x}, \hat{y}) \theta = (\hat{y}, \hat{x}) \) and \( (\hat{x}, \hat{y}) \sigma_f = (\hat{x} \oplus f(\hat{y}), \hat{y}) \). Also, \( \theta^2 \) and \( \sigma_f^2 \) are the identity transformation and therefore both are permutations. Thus, all DES-like-functions are permutations. Since \( \sigma_f = \delta_f \theta \) and \( \theta = \delta_f \theta \) where \( f(\hat{z}) = \theta^m \) for all \( \hat{z} \), it follows that the group of permutations generated by \( \theta \) and the set of all \( \sigma_f \)'s is identical with the group of permutations generated by the DES-like-functions, denoted \( \text{DES}_{2n} \).
(6) Define a 2-restricted DES-like-function on \( V_{2n} \) to be a DES-like-function \( \delta_f \) on \( V_{2n} \) determined by a function \( f: V_n \to V_n \), such that 
\[
f(2z) = g^{i-1}g(z_j, z_{j_2})^n \text{ for distinct } i, j_1, j_2 \text{ integers between 1 and } n \text{ and } g: V_2 \to V_2.
\]

3. THE MAIN RESULT

We shall prove first that for \( n \geq 1 \), DES\(_{2n}\) contains only even permutations. By Definition (5) and the discussion following it, it is sufficient to show that \( \sigma_f \) and \( \theta \) are even permutations.

Lemma 1: For any \( n > 1 \), \( \theta \) is an even permutation.

Proof: \( \theta \) exchanges, in pairs, a vector \((x, y)\) with the vector \((y, x)\) if \( x \neq y \) and leaves \( (x, x) \) invariant. Therefore \( \theta \) can be expressed by \((1/2)(2^n - 2^1) = 2^{n-1} \cdot (2^n - 1)\) transpositions, Thus, \( \theta \) is even.

Lemma 2: If \( n > 1 \), then for every \( f: V_n \to V_n \), \( \sigma_f \) is an even permutation.

Proof: Let \( \vec{0} \) denote the all-zero vector and \( #(f, \vec{0}) = |\{ z : f(z) = \vec{0} \}| \). If \( #(f, \vec{0}) = 2^n \) then \( \sigma_f \) is the identity permutation, which is an even permutation. Otherwise \( \sigma_f \) exchanges, in pairs, the vector \((\vec{x}, y)\) with the vector \((\vec{x} \oplus f(y), y)\) where \( f(y) \neq \vec{0} \); and therefore can be expressed by \((1/2) \cdot (2^n - #(f, \vec{0})) \cdot 2^n = 2^{n-1} \cdot (2^n - #(f, \vec{0}))\) transpositions. Since \( n > 1 \), this number is even.

Combining Lemmas 1 and 2, we see that, for \( n > 1 \), every permutation in DES\(_{2n}\) can be expressed by an even number of transpositions, hence:

Corollary 1: For every \( n > 1 \), DES\(_{2n}\) is a symmetric group of even permutations.
Denotation: Let $\sigma_{i,j}^e$ denote the permutation on $V_{2n}$ which exchanges, in pairs, the vector $(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_{j-1}, a_j, a_{j+1}, \ldots, a_{2n})$, $a_i \neq a_j$, with the vector $(a_1, \ldots, a_{i-1}, a_j, a_i, a_{i+1}, \ldots, a_{j-1}, a_i, a_{j+1}, \ldots, a_{2n})$.

Lemma 3: For any $1 \leq i \leq n$, $n < j \leq 2n$, $\sigma_{i,j}^e$ can be expressed as a sequential application of 2-restricted DES-like-functions.

Proof: Express $\sigma_{i,j}^e$ by the sequence $\delta_{f_1} \delta_{f_2} \delta_{f_1}^{f_0}$ where $f_1(z) = 0^{i-1}z(j-n)0^{n-i}$, $f_2(z) = 0^{(j-n)-1}z_10^{n-(j-n)}$ and $f_0(z) = 0^n$.

Lemma 4: For every $n > 1$, every 2-function on $V_{2n}$ can be expressed by a sequence of 2-restricted DES-like-functions.

Proof: With no loss of generality we consider only three cases in the proof of Lemma 4.

Denotation: Let $C[f;\{j_1,j_2\}+i]$ denote the 2-function on $V_{2n}$ determined by the Boolean function $f$ and the integers $j_1, j_2$, as follows:

$$(a_1, \ldots, a_i, \ldots, a_{2n})C[f;\{j_1,j_2\}+i] = (a_1, \ldots, a_i + f(a_j, a_{j+1}), \ldots, a_{2n}).$$

Case 1: $i \leq n$, $n < j_1, j_2 \leq 2n$. Express $C[f;\{j_1,j_2\}+i]$ by the sequence $\delta_{f_1}^{f_0} \delta_{f_2} \delta_{f_1}$ where $f_1(z) = 0^{i-1}f(z(j_1-n), z(j_2-n))0^{n-i}$ and $f_0(z) = 0^n$.

Case 2: $i, j_1, j_2 \leq n$. Express $C[f;\{j_1,j_2\}+i]$ by the sequence $\sigma_{j_1,j_1+n}^{ex} \sigma_{j_1,j_1+n}^{ex} \sigma_{j_2,j_2+n}^{ex} C[f;\{j_1+n,j_2+n\}+i] \sigma_{j_2,j_2+n}^{ex} \sigma_{j_1,j_1+n}^{ex}$.

According to Lemma 3 and Case 1, this sequence can be expressed by a sequence of 2-restricted DES-like-functions.
Case 3: \( i, j_1 \leq n, n < j_2 \leq 2n \). Express \( C_{[f: \{j_1, j_2\} \rightarrow i]} \) by the sequence 
\[
\circ_{j_1}^{\text{ex}} C_{[f: \{t, j_2\} \rightarrow i]} \circ_{j_1}^{\text{ex}} t,
\]
where \( t \) is chosen to be some integer such that \( t \neq j_2 \) and \( n < t \leq 2n \).

Again, according to Lemma 3 and Case 1, this sequence can be expressed by DES-like-functions.

Corollary 2: For \( n > 1 \) the group of permutations generated by all the \( 2 \)-restricted DES-like-functions on \( V_{2n} \) is equal to \( G_{2, 2n} \).

(Note that the set of \( 2 \)-restricted DES-like-functions on \( V_{2n} \) is a subset of the set of \( 2 \)-functions on \( V_{2n} \).)

Corollary 3: For every \( n > 1 \), \( \text{DES}_{2n} \supseteq G_{2, 2n} \).

Theorem 1:

(a) \( \text{DES}_2 = S_{V_2} \)

(b) For any \( n > 1 \), \( \text{DES}_{2n} = A_{V_{2n}} \).

Proof: The proof will be based on a theorem of Coppersmith and Grossman [1], (hereafter referred to as the CG-Theorem) stating that:

(i) If \( n \geq 4 \) and \( 2 \leq k \leq n-2 \), then \( G_{k, n} = A_{V_{n}} \).

(ii) For any \( n > 1 \), \( G_{n-1, n} = S_{V_{n}} \).

(iii) For any \( n > 1 \), \( G_{1, n} \) is a group of affine transformations on \( V_{n} \).

Fact (a) can be proven by directly computing \( \text{DES}_2 \) or by noting that \( \text{DES}_2 = G_{1, 2} \) and using CG-Theorem (ii).

Fact (b) can be proven by combining Corollaries 1 and 3 and CG-Theorem (i) yielding:

\[
A_{V_{2n}} \supseteq \text{DES}_{2n} \supseteq G_{2, 2n} \supseteq A_{V_{2n}}.
\]

Q.E.D.
Corollary 4: The group of permutations generated by the 2-restricted DES-like-functions on $V_{2n}$ is equal to DES$_{2n}$.

Remark: Note that the set of permutations generated by the DES is much smaller than $A_{V_{64}}$. This is due, mainly, to the fact that the DES performs 16 rounds while in the generation of DES$_{64}$ there is no restriction on the length of the sequence of DES-like-functions.

One can show that there exist permutations which require a sequence of length greater than $2^{32}$, and in general, at least of length $\log_2(2^{2n})!/n!\cdot 2^n$ (notice that the number of DES-like-functions is $2^n\cdot 2^n$).

Also, observe that a round in the DES realizes at most $2^{48}$ of the $2^{32}\cdot 2^{32}$ DES-like functions (on $V_{64}$) and that the functions applied in different rounds are related (due to the key schedule calculation).

4. GENERALIZATION

In this section we generalize the notion of DES-like-functions, introducing permutations which, when applied to a vector, operate on one part of it and permute the parts. We show that if the parts consist of more than one bit then these functions generate the Alternating Group.

The relevance of this result to the analysis of block-ciphers which operate on sub-blocks and permute the sub-blocks (such as the GDES-scheme [3]) is analogous to the relevance of Theorem 1 to the analysis of the DES.

Additional Definitions

(7) Let $G$ be a set of generators for $S_{\{1,2,\ldots,m\}}$. Denote by $\sigma_{\pi}^m, n = \sigma_f^m, n \cdot \sigma_{\pi}^m, n$ the permutation on $V_{m\cdot n}$ determined by the function $f$ and the permutation $\pi \in G$, such that
\[(x_1, x_2, \ldots, x_m)_{\sigma_{\pi}}^{m, n} = (x_1 \oplus f(x_2), x_2, \ldots, x_m), \]

and
\[(x_1, x_2, \ldots, x_m)_{\sigma_{\omega}}^{m, n} = (x_1\pi, x_2\pi, \ldots, x_m), \]

where for \(1 \leq i \leq m, x_i \in V_n\). We call the set \(\{\sigma_{\omega}^{m, n} : f \text{ is a } V_n + V_n \text{ function and } \pi \in G\}\) a Generalized Block Processor of \(m\) \(n\)-bit-long blocks and denote by \(GBP(m, n)\) the permutation group generated by it. Note that \(GBP(2, n) = \text{DES}_{2n}\).

(8) A 2-restricted GBP-function on \(V_{m \cdot n}\) is a permutation \(\sigma_{f, \pi}^{m, n}\) on \(V_{m \cdot n}\) determined by the function \(f: V_n \rightarrow V_n\), such that
\[f(z) = 0^{i-1} g(z_{j_1,j_2}) 0^{n-i}, \]

where \(i, j_1, j_2\) are distinct integers between 1 and \(n\) and \(g: V_2 \rightarrow V_1\).

(9) Let \(A\) be a binary \(n \times n\) non-singular matrix and \(b\) be a binary vector of length \(n\), we define the affine transformation of \(A\) and \(b\) to be the transformation \(\lambda_{A,b}\) on \(V_n\) determined by \(\lambda_{A,b} = A\lambda + b\), where the arithmetic is in the field \(\text{GF}(2)\).

**Theorem 2:** (a) For any \(n > 1, m > 1\) \(GBP(m; n) = A_{V_{m \cdot n}}\).

(b) For any \(m > 2\) \(GBP(m, 1)\) is the group of affine transformations on \(V_m\).

**Proof:** (a) Rephrase the lemmas such that Lemma 1 concerns \(\sigma_{\pi}^{m, n}\) and Lemma 2 concerns \(\sigma_{f, \pi}^{m, n}\). The extensions of Lemmas 1 and 2 yield \(GBP(m, n) \subseteq A_{V_{m \cdot n}}\). Extend the definition of \(\sigma_{i,j}^{\text{ex}}\) as follows: \(\sigma_{i,j}^{\text{ex}}\) is the permutation on \(V_{m \cdot n}\) which exchanges, in pairs, the vector
\[(a_1, a_2, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_j, \ldots, a_m, a_{m+1}, \ldots, a_{m+n}), a_i \neq a_j\],

with the vector
\[(a_1, a_2, \ldots, a_{i-1}, a_j, a_{i+1}, \ldots, a_j, \ldots, a_m, a_{m+1}, \ldots, a_{m+n}).\]

The rephrased Lemmas 3 and 4 concern the 2-restricted GBP-functions, and yield \(GBP(m, n) \subseteq G_{2, m \cdot n}\).

The extensions of Lemmas 1, 2, 3 are proven similarly to the way the Lemmas are proven in Sec. 3, however in the proof of the extension of Lemma 4...
additional cases may occur. Without loss of generality, we will consider the case of \( i \leq n, n \leq j_1 \leq 2n, 2n < j_2 \leq 3n \). \( \sigma^e_{j_2} \) can be applied to reduce this case to Case 1 of the proof of Lemma 4, where \( t \) is chosen such that \( t \neq j_1 \) and \( n < t \leq 2n \).

(b) Clearly, all \( \sigma_i^{m,1} \) and all \( \sigma_{m,1}^n \) are affine transformations. To show that every affine transformation can be expressed by \( \text{GBP}(m,1) \) we express the matrix \( A \) of the transformation as a product of elementary matrices. Given an affine transformation \( \lambda A, \vec{b} \) we can express it by the following sequence of affine transformations:

\[
\lambda A_1, \vec{0} \lambda A_2, \vec{0} \cdots \lambda A_q, \vec{0} \lambda I, \vec{b}_1, \lambda I, \vec{b}_2 \cdots \lambda I, \vec{b}_q
\]

where \( A_i \) is an elementary matrix, \( \vec{b}_j \) is a vector with one non-zero component, \( \vec{0} \) is the all-zero vector, \( I \) is the identity matrix, and \( A = A_q \lambda A_{q-1} \cdots A_1, \vec{b} = \vec{b}_1 + \vec{b}_2 + \cdots + \vec{b}_q \). It is easy to see that each of the transformations in the sequence can be expressed by a sequence of permutations in \( \text{GBP}(m,1) \).

Q.E.D.

It can be shown that every affine transformation on \( V_m \), where \( m > 2 \), is an even permutation on \( V_m \). Thus, (ii) implies that \( \text{GBP}(m,1) \subseteq A_m \) for \( m > 2 \). In fact this inclusion is proper.

Note that for \( m, n > 1 \), 2-restricted \( \text{GBP} \)-functions on \( V_{m \cdot n} \) generate \( A_{m \cdot n} \) and that the number of these 2-restricted \( \text{GBP} \)-functions is \( |G| \cdot (1+n(1+2+10\cdot n)) \).

ACKNOWLEDGEMENT

The authors wish to thank the referees for their valuable comments.
EPILOGUE

Following the suggestion of one of the referees, the authors are investigating the power of non-binary block ciphers. In these ciphers the messages and cryptograms are $q$-ary vectors of a fixed length $n$. Two of the results are:

1. For any $n \geq 6$, $2 \leq k \leq n-2$, $k$-functions on the vector space of dimension $n$ over $\mathbb{Z}_q$ (denoted $V_{q,n}$) generate $A_{V_{q,n}}$.

2. For every $m,n > 1$, such that $m \cdot n \geq 6$, any Generalized-Block-Processor of $m$ $q$-ary $n$-vectors generates $A_{V_{q,m \cdot n}}$ when $q$ is even or $(q-1) \cdot n \equiv 0 \pmod{4}$ otherwise it generates $S_{V_{q,m \cdot n}}$. 
REFERENCES

