Permutation Generators of Alternating Groups

Josef Pieprzyk
Xian-Mo Zhang
Department of Computer Science
University of Wollongong
Wollongong, NSW 2522, Australia
josef,xianmo@cs.uow.edu.au

Abstract

using elementary permutations, also called modules. These modules have a simple structure and are based on internal smaller permutations. Two cases are considered. In the first, the modules apply internal permutations only. It has been proved that the composition of modules generates the alternating group for the number of binary inputs bigger than 2. In the second, DES-like modules are considered and it is shown that for a large enough number of binary inputs, they produce the alternating group, as well.

1 Introduction

Coppersmith and Grossman in [**?**] studied generators for certain alternating groups. They defined k-functions which create corresponding permutations. Each k-function along with its connection topology produces a single permutation which can be used as a generator. The authors proved that these generators produce at least alternating groups using a finite number of their compositions. It means that with generators of relatively simple structure, it is possible to produce at least half of all the permutations using composition.

There is one problem with such generators - they do not have a fixed connection topology. The well-known DES encryption algorithm applies the fixed connection topology. The 64-bit input is divided into halves. The right hand half is used as the input (after the expansion operation) for the eight different S-boxes each of which transforms the 6-bit input into the 4-bit output. The resulting 32-bit string is added modulo 2 to the corresponding bits of the second half. Next the halves are swopped. Even and Goldreich [**?**] proved that the DES-like connection topology along with k-functions can also generate alternating groups.

This raises the following question: *Is it possible to generate the alternating groups when k-permutations are used instead of k-functions ?*

2 Background and Notations

Symmetric enciphering algorithms operate on fixed size blocks of binary strings. We assume that the length of the block is N bits, and for a fixed key, algorithms give permutations from the set of 2^N possible elements. The vector space of dimension N over $GF(2)$ contains all binary strings of length N and is denoted as V_N. The following notations will be used throughout this chapter:

$\mathbf{S}_X$ - the group of all permutations on a set X,
$\mathbf{S}_{V_N}$ - the group of all permutations on V_N (it consists of $2^N!$ elements),
$\mathbf{A}_{V_N}$ - the alternating group of all permutations on V_N (it has $1/2(2^N!)$ elements).

The following definition describes k-permutations and can be seen as a modification of the definition given by Coppersmith and Grossman [**?**].

Definition 1 *Let $1 \leqq k \leqq (N/2)$. By a k-permutation on V_N, we mean a permutation σ of V_N determined by a subset of order $2k$, $\{i_1, \ldots, i_k, j_1, \ldots, j_k\} \subseteq \{1, \ldots, N\}$ and a permutation*

$$p : V_N \longrightarrow V_N \tag{1}$$

as follows:

$$\begin{array}{lcll} ((a_1, \ldots, a_N)\sigma)_m & = & a_m & \text{for } m \in \{i_1, \ldots, i_k\} \\ ((a_1, \ldots, a_N)\sigma)_m & = & a_m \oplus p(a_{i_1}, \ldots, a_{i_k})_m & \text{for } m \in \{j_1, \ldots, j_k\} \end{array}$$

3 Structure without Topology Restrictions

In this section we refer to the results obtained by Coppersmith and Grossman [**?**]. The k-permutation for a fixed k is the basic module which is used to create our encryption system. Clearly, k-permutations on V_N generate a subgroup of $\mathbf{S}_{V_N}$ and the subgroup is denoted as $\mathbf{P}_{k,N} \subset \mathbf{S}_{V_N}$.

Lemma 1

$$\mathbf{P}_{1,2} = \mathbf{S}_{V_2} \tag{2}$$

Proof. There are four possible modules and they produce the following permutations:

$$\begin{array}{lcllcl} g_1 & = & (0,3,2,1) & = & (0)(2)(1,3) \\ g_2 & = & (2,1,0,3) & = & (1)(3)(0,2) \\ g_3 & = & (1,0,3,2) & = & (0,1)(2,3) \\ g_4 & = & (0,1,3,2) & = & (0)(1)(2,3) \end{array}$$

The above permutations are written in two different ways. The first uses the standard notation which for g_1 is as follows:

$$g_1(0) = 0; g_1(1) = 3; g_1(2) = 2; g_1(3) = 1.$$

The second one applies the reduced cyclic form (see Wielandt [**?**] pages 1 and 2). It is easy to check that the permutations generate $\mathbf{S}_{V_2}$. □

Lemma 2 *The 2-permutations generate subgroup $\mathbf{P}_{2,4} \subset \mathbf{S}_{V_4}$ whose coordinates are affine.*

Proof. Observe that the permutation $p : V_2 \longrightarrow V_2$ must always have linear coordinates. □

Lemma 3 *For $k \geqq 3$,*

$$\mathbf{P}_{k,2k} = \mathbf{A}_{V_{2k}}. \tag{3}$$

Proof. First we prove that $\mathbf{P}_{3,6} = \mathbf{G}_{2,6}$ (note that $\mathbf{G}_{2,6}$ is defined as in [**?**] and means the subgroup of $\mathbf{S}_{V_N}$ generated by the *2*-functions). It is always possible to generate any $\mathbf{G}_{2,6}$ module by composition of a finite number of *3*-permutation modules. For example, assume that we would like to obtain a *2*-function module over 6 binary variables $(x_1, x_2, x_3, x_4, x_5, x_6)$ which transforms input

$$(x_1, x_2, x_3, x_4, x_5, x_6) \longrightarrow (x_1, x_2, x_3, x_4 \oplus x_1 x_2, x_5, x_6) \tag{4}$$

Applying the composition of two *3*-permutation modules whose coordinates are given in the table below, we obtain the required *2*-function module.

x_1, x_2, x_3	*First Module* f_1, f_2, f_3	*Second Module* g_1, g_2, g_3	*Composition* $f_1 \oplus g_1, f_2 \oplus g_2, f_3 \oplus g_3$
000	110	110	000
001	111	111	000
011	100	100	000
010	101	101	000
110	011	010	001
111	010	011	001
101	000	000	000
100	001	001	000

The example can easily be extended for arbitrary case. It means that:

$$\mathbf{P}_{3,6} \supseteq \mathbf{G}_{2,6} = \mathbf{A}_{V_6}$$

Using Coppersmith and Grossman theorem [**?**] (referred to as the C-G theorem), it is obvious that:

$$\mathbf{P}_{3,6} \subseteq \mathbf{G}_{2,6} = \mathbf{A}_{V_6}$$

Combining the two inclusions, we get the final result :

$$\mathbf{P}_{3,6} = \mathbf{A}_{V_6} \tag{5}$$

In general, the C-G theorem and properties of k-permutations allow us to write the following sequence of inclusions:

$$\begin{array}{ccccccc} \mathbf{A}_{v_{2k}} & \subseteq & \mathbf{G}_{2,2k} & \subseteq & \mathbf{P}_{3,2k} & & \\ & \subseteq & \mathbf{P}_{k,2k} & \subseteq & \mathbf{G}_{k,2k} & \subseteq & \mathbf{A}_{V_{2k}} \end{array}$$

where $k \geqq 3$ and it proves the lemma. □

The proved lemma and the C-G theorem allow us to formulate the following theorem.

Theorem 1 *The group generated by* $\mathbf{P}_{k,2k}$ *is:*

- *the group* $\mathbf{S}_{V_2}$ *for* $k = 1$,
- *the subgroup of affine transformations for* $k = 2$,
- *the group* $\mathbf{A}_{V_{2k}}$ *for* $k \geqq 3$.

The theorem can be easily generalized (the proof is omitted).

Theorem 2 *Let* $N \geqq 2k$. *The group generated by* $\mathbf{P}_{k,N}$ *is:*

- *the subgroup of affine transformations for* $k = 2$,
- *the group* $\mathbf{A}_{V_N}$ *for* $k \geqq 3$.

4 DES Structure

An interesting question is how the structure of the well-known DES algorithm [**?**] limits the permutation group generated by DES-like functions on V_{2k}. Even and Goldreich [**?**] proved that the DES-like functions generate the alternating group for $k > 1$ and the whole permutation group for $k = 1$. In this section we are going to examine a case when the DES is based on permutations that is, the S-boxes realize one-to-one transformations (the existing S-boxes provide the inverible mapping of 6-bit input into 4-bit output).

Definition 2 *The DES-like permutation σ on V_{2k} is defined by a composition of two modules:*

- *the first module is determined by permutation $p : V_k \longrightarrow V_k$ and transforms the input $(x_1, \ldots, x_{2k}) \in V_{2k}$ into:*

$$(x_1 \oplus p_1(x_{k+1}, \ldots, x_{2k}), \ldots, x_k \oplus p_k(x_{k+1}, \ldots, x_{2k}), x_{k+1}, \ldots, x_{2k})$$

  where $(p_1, \ldots, p_k)$ are coordinates of $p(x_{k+1}, \ldots, x_{2k})$,

- *the second module swops the vector:*

$$(x_1, \ldots, x_k, x_{k+1}, \ldots, x_{2k})$$

  with the vector

$$(x_{k+1}, \ldots, x_{2k}, x_1, \ldots, x_k).$$

The group generated by DES-like permutations is denoted by DESP_{2k} *($\mathrm{DESP}_{2k} \subset S_{V_{2k}}$).*

Lemma 4

$$\mathrm{DESP}_2 = \mathbf{A}_{V_2} \tag{6}$$

There are two possible permutations σ_1 and σ_2 generated by $p_1(x_2) = x_2$ (the identity permutation) and $p_2(x_2) = \bar{x}_2$ (the negation permutation), respectively and

$$\begin{aligned} \sigma_1 &= (0)(1,2,3) \\ \sigma_2 &= (0,1,2)(3) \end{aligned}$$

It is easy to check that the two permutations generate $\mathbf{A}_{V_2}$. $\diamond$

Lemma 5 *The permutation $\theta_4 \in \mathbf{A}_{V_4}$ that swops (x_1, x_2, x_3, x_4) into (x_3, x_4, x_1, x_2) can be expressed by composition of DES-like permutations.*

Proof. First note that

$$\begin{aligned} \theta_4 &= (0,4,8,12,1,5,9,13,2,6,10,14,3,7,11,15) \\ &= (1,4)(2,8)(3,12)(6,9)(7,13)(11,14) \end{aligned}$$

We shall show that θ_4 may be obtained using the composition of the following four DES-like permutations:

$$\begin{aligned} g_1 &= (0,5,10,15,1,4,11,14,2,7,8,13,3,6,9,12) \\ &\quad \text{for } p(x_3, x_4) = I = (0,1,2,3) \\ g_2 &= (0,6,9,15,1,7,8,14,2,4,11,13,3,5,10,12) \\ &\quad \text{for } p(x_3, x_4) = (0,2,1,3) \\ g_3 &= (0,6,11,13,1,7,10,12,2,4,9,15,3,5,8,14) \\ &\quad \text{for } p(x_3, x_4) = (0,2,3,1) \\ g_4 &= (0,7,9,14,1,6,8,15,2,5,11,12,3,4,10,13) \\ &\quad \text{for } p(x_3, x_4) = (0,3,1,2) \end{aligned}$$

where $p(x_3, x_4)$ are permutations of four binary elements 0,1,2,3 (coded 00,01,10,11). We create 3 intermediate permutations as follows:

$$\begin{aligned}
\alpha &= g_2^{-1} \circ g_1 \\
&= (0,13,14,3,4,9,10,7,8,5,6,11,12,1,2,15) \\
&= (1,13)(2,14)(5,9)(6,10); \\
\beta &= g_3^3 \circ \alpha \circ g_3^{-3} \\
&= (0,4,2,6,1,5,3,7,8,12,10,14,9,13,11,15) \\
&= (1,4)(3,6)(9,12)(11,14); \\
\gamma &= g_4^3 \circ \alpha \circ g_4^{-3} \\
&= (0,1,8,9,4,5,12,13,2,3,10,11,6,7,14,15) \\
&= (2,8)(3,9)(6,12)(7,13);
\end{aligned}$$

and the composition of the last two is:

$$\begin{aligned}
\gamma \circ \beta &= (0,4,8,12,1,5,9,13,2,6,10,14,3,7,11,15) \\
&= (1,4)(2,8)(3,12)(6,9)(7,13)(11,14).
\end{aligned}$$

□

Lemma 6 *The permutation $\theta_6 \in \mathbf{A}_{V_6}$ which swops:*

$$(x_1, x_2, x_3, x_4, x_5, x_6) \rightarrow (x_4, x_5, x_6, x_1, x_2, x_3) \tag{7}$$

can be expressed by composition of DES-like permutations.

Proof. Any DES-like permutation from S_{V_6} transforms the input sequence

$$(x_1, x_2, x_3, x_4, x_5, x_6) \tag{8}$$

into

$$(x_4, x_5, x_6, x_1 \oplus p_1(x_4, x_5, x_6), x_2 \oplus p_2(x_4, x_5, x_6), x_3 \oplus p_3(x_4, x_5, x_6)), \tag{9}$$

where the permutation $p(x_4, x_5, x_6) = (p_1, p_2, p_3)$. We simplify our considerations choosing the permutation $p(x_4, x_5, x_6) = (x_4, p_2(x_5, x_6), p_3(x_5, x_5))$. So, we can independently consider two DES-like permutations. First one σ transforms the sequence (x_1, x_4) into $(x_4, x_1 \oplus x_4)$ and generates the identity permutation after three compositions ($\sigma^3 = I$). The second permutation $\sigma_g : V_4 \rightarrow V_4$ belongs to $DESP_4$. If we select the same sequence of permutations as in the previous Lemma, we can obtain:

$$(x_2, x_3, x_5, x_6) \rightarrow (x_5, x_6, x_2, x_3) \tag{10}$$

This can be done using 22 compositions (observe that $g_2^{-1} = g_2^5$; $g_3^{-3} = g_3^2$; $g_4^{-3} = g_4^2$). Therefore after 66 compositions it is possible to obtain

$$(x_1, x_2, x_3, x_4, x_5, x_6) \rightarrow (x_1, x_5, x_6, x_4, x_2, x_3) \tag{11}$$

By repeating the process three times, we get

$$\begin{array}{cccccc}
(x_1, & x_2, & x_3, & x_4, & x_5, & x_6) \\
 & & \downarrow & & & \\
(x_4, & x_2, & x_5, & x_1, & x_3, & x_6) \\
 & & \downarrow & & & \\
(x_3, & x_2, & x_6, & x_1, & x_4, & x_5) \\
 & & \downarrow & & & \\
(x_3, & x_4, & x_5, & x_1, & x_3, & x_2)
\end{array}$$

To obtain the DES swopping operation, we need to exchange bits x_3 and x_2. This can be done using the product of the following permutations:

$$\delta \circ \gamma \circ \beta = (1,2)(5,6)(9,10)(13,14) \tag{12}$$

where:

$$\begin{aligned} \beta &= g_1^2 \circ \alpha \circ g_1; \\ \gamma &= g_3^2 \circ \alpha \circ g_3^4; \\ \delta &= g_2^5 \circ g_4 \circ g_2; \\ \alpha &= g_6^4 \circ g_5; \end{aligned}$$

and:

$$\begin{aligned} g_1 &= (0,5,10,15,1,4,11,14,2,7,8,13,3,6,9,12) \\ &\quad \text{for } p(x_3,x_4) = I = (0,1,2,3); \\ g_2 &= (0,5,11,14,1,4,10,15,2,7,9,12,3,6,8,13) \\ &\quad \text{for } p(x_3,x_4) = (0,1,3,2); \\ g_3 &= (0,6,9,15,1,7,8,14,2,4,11,13,3,5,10,12) \\ &\quad \text{for } p(x_3,x_4) = (0,2,1,3); \\ g_4 &= (1,4,10,15,0,5,11,14,3,6,8,13,2,7,9,12) \\ &\quad \text{for } p(x_3,x_4) = (1,0,2,3); \\ g_5 &= (3,4,9,14,2,5,8,15,1,6,11,12,0,7,10,13) \\ &\quad \text{for } p(x_3,x_4) = (3,0,1,2); \\ g_6 &= (3,5,8,14,2,4,9,15,1,7,10,12,0,6,11,13) \\ &\quad \text{for } p(x_3,x_4) = (3,1,0,2). \end{aligned}$$

To leave other positions unchanged, it is necessary to apply the above sequence of permutations three times. □

Theorem 3 *The group* DESP_{2k} *generated by DES-like permutations is:*

(a) *the alternating group* $\mathbf{A}_{V_2}$ *for* $k = 1$,

(b) *the group of affine transformations for* $k = 2$,

(c) *the alternating group* $\mathbf{A}_{V_{2k}}$ *for* $k \geqq 3$.

Proof. The statement (a) has been proved in the lemma 4. According to the lemmas 5 and 6 each swopping module can be expressed as a composition of DES-like permutations for $k \geqq 2$. It means that any permutation from $\mathbf{P}_{k,2k}$ may be represented by a composition of DES-like permutations, i.e.:

$$DESP_{2k} \supseteq \mathbf{P}_{k,2k}. \tag{13}$$

Considering the theorem proved by Even and Goldreich [**?**] (referred to as the E-G theorem), the following inclusion holds:

$$DESP_{2k} \subseteq DES_{2k} = \mathbf{A}_{V_{2k}} \text{ for } k \geqq 3 \tag{14}$$

where DES_{2k} is a group generated by DES-like functions given in [**?**]. Taking 13 and 14, we obtain the statement (c). The statement (b) is obvious. □

5 Conclusions

When designing new cryptographic algorithms, we face the problem of selecting the algorithm structure (or the connection topology). Results by Coppersmith and Grossman [**?**], Even and Goldreich [**?**] proved that the DES structure is flexible enough as a composition of DES iterations can generate the suitable alternating group while the number of iterations is not limited (the DES uses 16 ones) and functions in S-boxes are not fixed (i.e.they can be freely selected for each iteration).

In this work we have answered the problem of what happens if S-boxes realize one-to-one mapping (the current S-boxes in the DES are one-to-many). Astonishingly, the structure with one-to-one S-box transformations does not restict the number of possible permutations obtained using the composition if only the number of inputs/outputs is equal to or larger than 6 (or $k \geqq 3$).

Each iteration may be considered as a generator of the alternating group. We have simply proved that having $(2^{N/2})!$ generators we can produce $(2^N)!$ different permutations. From a practical point of view we would like to have a smaller set of generators. Bovey and Williamson reported in [**?**] that a ordered pair of generators can produce either $\mathbf{A}_{V_N}$ or $\mathbf{S}_{V_N}$ with the probability greater than $1 - exp(-log^{1/2}2^N)$. So if we select the pair at random, there is a high probability that it generates at least $\mathbf{A}_{V_N}$. However, we would not like to rely on the probability theory. Instead, we would like to know for certain that the set of generators is complete, i.e. that it generates either $\mathbf{A}_{V_N}$ or $\mathbf{S}_{V_N}$.

There remain the following open problem:

- Are the DES generators complete (considering the current S-box structure) ?