J. Cryptology (1994) 7: 61–65

Journal of
CRYPTOLOGY

A Weak Cipher that Generates the Symmetric Group

Sean Murphy, Kenneth Paterson, and Peter Wild
Information Security Group, Royal Holloway and Bedford New College,
University of London, Egham, Surrey TW20 0EX, England

Communicated by Dan Coppersmith

Received 12 February 1993

Abstract. There has been recent interest in the permutation group generated by the round functions of a block cipher. In this paper we present a cautionary example of a block cipher which generates the full symmetric group yet is very weak.

Key words. Block cipher, Permutation group.

1. Introduction

We consider iterated block ciphers in which each round of a block cipher is a permutation of the message space determined by the subkey used in that round. The group generated by the set of possible round permutations acting on the message space is of obvious cryptographic interest. For example, if this group is too small, then the cryptosystem obtained by iterating the round function may be vulnerable to attack. This group was first studied by Coppersmith and Grossman [1]. Further interest in the group properties of block ciphers has been stimulated by Wernsdorf [4], who showed that the DES round functions generate the large simple group $A_{2^{64}}$, which acts primitively on the message space of 64-bit blocks. More recently, Magliveras and Memon [3] have considered the group properties of a cryptosystem based on permutation groups. They claim that the ability of their system to generate the symmetric group on the message space is "one of the strongest security conditions that can be offered".

In this paper we present an example of a cipher whose round functions generate the full symmetric group yet is very weak. The conclusion (unsurprisingly) is that the group-theoretic properties of a block cipher should not be taken in isolation as a measure of cryptographic strength. This is analogous to the situation in stream-cipher design where no single measure of complexity is sufficient to guarantee the unpredictability of the keystream.

This paper is organized in the following manner. In Section 2 we define the round functions of our cipher and show that they generate the symmetric group. In Section 3 we present a known plaintext attack on the cipher that requires only one

plaintext–ciphertext pair. In Section 4 we consider an r-round cipher using the round function of Section 2, and we show that such a cipher generates either the symmetric group or the alternating group depending on whether r is odd or even. Finally, in Section 5, we draw some conclusions.

2. The Round Functions and Their Group

For $n > 3$, let V_n denote the vector space of dimension n over $\mathbf{Z}_2$. Thus the elements of V_n are binary n-tuples. We denote an n-tuple by the corresponding number in the range $0, \ldots, 2^n - 1$. We take our message space, M, and subkey space, K (for each round), both to be V_n. The one-round functions E_k: $M \to M$ are defined, for $k \in K$, by

$$mE_k = (m \oplus k)\theta,$$

where $\oplus$ denotes bitwise XOR and θ is the following permutation of V_n:

$$\theta = (1, 2, \ldots, 2^{n-1} - 1, 2^{n-1} + 1, \ldots, 2^n - 3, 2^n - 2, 2^{n-1}) \in S_{2^n}.$$

Thus θ is a $(2^n - 2)$-cycle and has 0 and $(2^n - 1)$ as fixed points. Let G denote the subgroup of S_{2^n} generated by $\{E_k | k \in K\}$.

Lemma 1. *G is transitive on V_n.*

Proof. Let x, y be arbitrary elements of V_n. Then $xE_a = y$, where $a = y\theta^{-1} \oplus x$. □

Let G_0 denote the stabilizer of 0. Thus, $G_0 = \{g \in G | 0g = 0\}$, and we have the following result.

Lemma 2. *G_0 is transitive on $V_n \backslash \{0\}$.*

Proof. Clearly, E_0^i fixes 0 for any power i, and so $E_0^i \in G_0$ for any power i. Now, θ is a $(2^n - 2)$-cycle, so, for arbitrary elements x, $y \neq 2^n - 1$ of $V_n \backslash \{0\}$, a power i exists such that $x\theta^i = y$, and so $xE_0^i = y$. Thus we have shown that, for any $x, y \neq 0, 2^n - 1$, an element $g \in G_0$ exists such that $xg = y$.

Now, $E_1 E_2 \in G_0$, since

$$(0)E_1 E_2 = (1)\theta E_2 = 2E_2 = (0)\theta = 0,$$

and therefore $E_1 E_2 E_0^i \in G_0$ for any power i. However,

$$(2^n - 1)E_1 E_2 = (2^n - 2)\theta E_2 = (2^{n-1})E_2 = (2^{n-1} + 2)\theta \neq 0, 2^n - 1 \qquad (n > 3).$$

Hence for any $x \neq 0, 2^n - 1$, there is a power i such that $(2^n - 1)E_1 E_2 E_0^i = x$, and it thus follows that G_0 is transitive on $V_n \backslash \{0\}$. □

From Lemmas 1 and 2, we can immediately deduce the following.

Corollary 1. *G is 2-transitive on V_n.*

We now prove the final lemma needed to establish that these round functions generate the symmetric group.

Lemma 3. *G contains the transposition $(0, 2^n - 1)$.*

Proof. We have $E_0 = \theta$ and $mE_{2^{n-1}} = (m \oplus 2^{n-1})\theta$. *Thus*

$$E_0 = \theta = (1, 2, \ldots, 2^{n-1} - 1, 2^{n-1} + 1, \ldots, 2^n - 3, 2^n - 2, 2^{n-1}),$$

$$E_{2^{n-1}} = (0, 1, 2^{n-1} + 2, 3, 2^{n-1} + 4, \ldots, 2^{n-1} - 3, 2^n - 2, 2^{n-1} - 1,$$
$$2^n - 1, 2^{n-1} + 1, 2, 2^{n-1} + 3, 4, \ldots, 2^n - 3, 2^{n-1} - 2, 2^{n-1}),$$

so E_0 is a $(2^n - 2)$-cycle and $E_{2^{n-1}}$ is a 2^n-cycle. Now,

$$E_0^{2^{n-1}-1} = (1, 2^{n-1} + 1)(2, 2^{n-1} + 2)\cdots(2^{n-1} - 2, 2^n - 2)(2^{n-1} - 1, 2^{n-1}),$$

$$E_{2^{n-1}}^{2^{n-1}} = (0, 2^n - 1)(1, 2^{n-1} + 1)(2, 2^{n-1} + 2)\cdots(2^{n-1} - 2, 2^n - 2)(2^{n-1} - 1, 2^{n-1}).$$

Multiplying these two elements together gives us

$$E_{2^{n-1}}^{2^{n-1}} E_0^{2^{n-1}-1} = (0, 2^n - 1) \in G. \qquad \square$$

We now prove the main result about this cipher, namely, that the round functions generate the full symmetric group on V_n.

Theorem 1. $G = S_{V_n} = S_{2^n}$.

Proof. Clearly, $G \leq S_{V_n}$. However, we have shown that G is 2-transitive and contains a transposition, so G contains all transpositions. The set of transpositions on V_n generate the symmetric group on V_n, a set of size 2^n. $\square$

3. Cryptanalysis

Clearly, as a cryptosystem, these one-round functions are weak. Given a corresponding message and ciphertext pair (m, c), we can easily find key k since $k = m \oplus c\theta^{-1}$. However, many block ciphers are built from iterations of weak functions. Consider $F_{\mathbf{k}} = E_{k_1} \cdots E_{k_r}$, the r-round iterated block cipher consisting of encryption functions E_{k_i}, where $k_1, \ldots, k_r$ are independent n bit subkeys. Thus the key of this iterated block cipher is $(k_1, \ldots, k_r)$, so the key space is of size 2^{nr}. We have seen that this is a cipher whose round functions generate S_{2^n}, so it is a candidate for a good cipher. We show that this is not the case.

Let $x^{(i)}$ denote the ith most significant bit of $x \in V_n$, so $x^{(1)}$ denotes the left-hand bit of x, etc. It can be clearly seen that $(x\theta)^{(1)} = x^{(1)}$ unless $x = 2^{n-1} - 1, 2^{n-1}$. Thus $(x\theta)^{(1)} = x^{(1)}$ with probability $(1 - 2^{-(n-1)})$. Generally,

$$(x\theta)^{(i)} = x^{(i)} \qquad \text{with approximate probability } (1 - 2^{i-n}) \qquad (i < n),$$

and so

$$(xE_k)^{(i)} = (x \oplus k)^{(i)} \qquad \text{with approximate probability } (1 - 2^{i-n}) \qquad (i < n).$$

If we consider the iterated cipher, then we have, for $i < n$,

$$(xF_{\mathbf{k}})^{(i)} = (xE_{k_1} \cdots E_{k_r}) = (x \oplus k_1 \oplus \cdots \oplus k_r)^{(i)} \qquad \text{with probability } \geq (1 - 2^{i-n})^r.$$

If we know one plaintext–ciphertext pair, (m, c) where $c = mF_{\mathbf{k}}$, then we know the bit of key information $(k_1 \oplus \cdots \oplus k_r)^{(i)}$ with probability $(1 - 2^{i-n})^r$, that is, for reasonably large n, moderate r, and most i, with near certainty. If we knew many pairs of plaintext and ciphertext, we would be able to determine key bits much more accurately. Moreover, if we know $(k_1 \oplus \cdots \oplus k_r)^{(i)}$, then, for any ciphertext block, we know that the corresponding plaintext block must be $m^{(i)} = c^{(i)} \oplus (k_1 \oplus \cdots \oplus k_r)^{(i)}$ with probability $(1 - 2^{i-n})^r$.

4. The Group Generated by the r-Round Encryption Function

Although Wernsdorf [4] showed that the round functions of DES generated the alternating group $A_{2^{64}}$, as he pointed out, it is not known if the full 16-round DES generates the alternating group. In this section we demonstrate that the r-round iterated cipher described above generates either the symmetric or the alternating group on 2^n letters if r is respectively odd or even. We proceed in a similar way to Section 2. Thus, let $G^{(r)}$ denote the group generated by such an r-round cipher, and let $G_0^{(r)}$ denote the stabilizer of 0 in $G^{(r)}$.

Lemma 4. *$G^{(r)}$ is transitive on V_n.*

Proof. Given $x, y \in V_n$, $xE_xE_0^{r-2}E_{y\theta^{-1}} = y$, and $E_xE_0^{r-2}E_{y\theta^{-1}} \in G^{(r)}$. □

Lemma 5. *$G_0^{(r)}$ is transitive on $V_n \backslash \{0\}$.*

Proof. Given $x \neq 0, 2^n - 1$, there is $g_x \in G_0^{(r)}$ such that $(2^n - 1)g_x = x$, where $g_x = E_0^{sr-i_x-2}E_1E_2E_0^{i_x} \in G_0^{(r)}$ for some power i_x and suitable s. Similarly, for $y \neq 0, 2^n - 1$, there is $g_y \in G_0^{(r)}$ such that $(2^n - 1)g_y = y$. Thus $g_x^{-1}g_y \in G_0^{(r)}$ and $xg_x^{-1}g_y = y$. □

Corollary 2. *$G^{(r)}$ is 2-transitive on V_n.*

Theorem 2. *For r odd, $G^{(r)} = S_{2^n}$.*

Proof. From the proof of Theorem 1, we have, for r odd, $(E_{2^{n-1}}^{2^{n-1}}E_0^{2^{n-1}-1})^r = (0, 2^n - 1) \in G^{(r)}$. $G^{(r)}$ is 2-transitive and contains a transposition, so $G^{(r)} = S_{2^n}$. □

Theorem 3. *For r even, $G^{(r)} = A_{2^n}$.*

Proof. We first show that a one-round encryption is an odd permutation. Recall that a one-round function is defined by $(m)E_k = (m \oplus k)\theta$. If $k \neq 0$, then the XOR with k is a product of 2^{n-1} transpositions, so is an even permutation, and the XOR with 0 gives the identity permutation. θ is a $(2^n - 2)$-cycle, so is an odd permutation. Thus any one-round function, E_k, is an odd permutation. Hence an encryption

function consisting of an even number of rounds is the product of an even number of odd permutations and hence is an even permutation, so $G^{(r)} < A_{2^n}$.

We now show that $G^{(r)}$ contains all 3-cycles, by showing that $G^{(r)}$ contains an arbitrary 3-cycle. Let $x, y, z \in V_n$, then, since 1 and $(r-1)$ are odd, $g = (x, y) \in G^{(1)}$ and $h = (x, z) \in G^{(r-1)}$. If g is an l-round encryption and h is an $m(r-1)$-round encryption, then both l and m are odd, since otherwise we would have an odd permutation as an even-round encryption function. Now, $g^m h^l$ is an mlr-round encryption, so $g^m h^l = (x, y, z) \in G^{(r)}$. Thus $G^{(r)}$ contains all 3-cycles, and so $G^{(r)} = A_{2^n}$. □

5. Conclusions

Magliveras and Memon [3] indicate their belief that the property of generating the symmetric group on the message space is "one of the strongest security conditions that can be offered". Our example of a weak system whose group is all of S_{2^n} is evidence against this belief. Further evidence that a large group is not an indicator of strength is the fact, already noted by Even and Goldreich [2], that even though the round functions generate a large group, most permutations in this large group require the composition of an enormous number of round functions.

In his conclusions, Wernsdorf [4] indicates more refined properties that the group G should have in order to "exclude several imaginable crytanalytic shortcuts", namely, that G should be large, simple, and act primitively on the message space. We have shown that these conditions are not sufficient for security. Our weak cryptosystem's round function generates a group, S_{2^n}, that has a large simple normal subgroup, A_{2^n}, which acts primitively on the message space. Although our example is contrived, it is conceivable that a more realistic system could be designed to have desirable group properties but which is weak.

References

[1] D. Coppersmith and E. Grossman. Generators for certain alternating groups with applications to cryptology. *SIAM Journal of Applied Mathematics*, **29**: 624–627, 1975.

[2] S. Even and O. Goldreich. DES-like functions can generate the alternating group. *IEEE Transactions on Information Theory*, **29**: 863–865, 1983.

[3] S. S. Magliveras and N. D. Memon. Algebraic properties of cryptosystem PGM. *Journal of Cryptology*, **5**: 167–184, 1992.

[4] R. Wernsdorf. The one-round functions of DES generate the alternating group. *Advances in Cryptology—EUROCRYPT 92 Proceedings*, Lecture Notes in Computer Science, Vol. 658, Springer-Verlag, Berlin, 1993, pp. 99–112.