Is DES a Pure Cipher?
(Results of More Cycling Experiments on DES)[1]

(Preliminary Abstract)

Burton S. Kaliski Jr., Ronald L. Rivest, and Alan T. Sherman

MIT Laboratory for Computer Science
545 Technology Square
Cambridge, MA 02139
December 1985

Abstract

During summer 1985, we performed eight cycling experiments on the Data Encryption Standard (DES) to see if DES has certain algebraic weaknesses. Using special-purpose hardware, we applied the cycling closure test described in our Eurocrypt 85 paper to determine whether DES is a pure cipher. We also carried out a stronger version of this test. (A cipher is *pure* if, for any keys i, j, k, there exists some key l such that $T_i T_j^{-1} T_k = T_l$, where T_w denotes encryption under key w.) In addition, we followed the orbit of a randomly chosen DES transformation for 2^{36} steps, as well as the orbit of the composition of two of the "weak key" transformations. Except for the weak key experiment, our results are consistent with the hypothesis that DES acts like a set of randomly chosen permutations. In particular, our results show with overwhelming confidence that DES is not pure. The weak key experiment produced a short cycle of about 2^{33} steps, the consequence of hitting a fixed point for each weak key.

Key Words and Phrases

Birthday Paradox, closed cipher, cryptanalysis, cryptography, cryptology, cycle-detection algorithm, Data Encryption Standard (DES), finite permutation group, idempotent cryptosystem, multiple encryption, pure cipher.

[1]This research is supported by NSF grant MCS-8006938 and IBM.

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 212-226, 1986.

1 Introduction

At the Eurocrypt 85 conference, we presented experimental statistical evidence that the set of DES transformations is not closed under functional composition [KRS85].[2] During May to August 1985, we performed additional experiments to determine if DES has certain other related algebraic weaknesses. In particular, we addressed the open question, "Is DES a pure cipher?"[3] In addition, we performed a strengthened version of our closure test and we ran two experiments to investigate the order of DES transformations. Using a combination of software and special-purpose hardware, we carried out eight experiments, covering five different algebraic tests. Although we experimented only with DES, our tests are general in nature and apply to any to finite, deterministic cryptosystem.

None of our experiments involving randomly chosen DES transformations detected any algebraic weaknesses. In particular, our data show with extremely high confidence that DES is not pure. However, one experiment inadvertently discovered fixed points for two of the keys, thereby revealing a previously unpublished additional weakness of the weak keys [Dav82].

This abstract is organized in four sections. Section 1 gives an overview of our experiments and explains the purpose of our tests. Section 2 introduces the notation and terminology used throughout the abstract and summarizes previous cycling studies on DES. Section 2 also briefly reviews the cycling closure test and describes our hardware implementation of it. Section 3 lists concise descriptions of our algebraic tests. Finally, section 4 summarizes our findings and explains the two interesting structural properties that we encountered during our tests. An appendix which describes our detailed experimental results is also included.

1.1 Overview and Motivation

It is important to know if DES is pure for essentially the same reasons that it is important to know if DES is closed. If DES were pure, then Tuchman's multiple encryption scheme would be equivalent to single encryption, and DES would be vulnerable to a known-plaintext attack that runs in 2^{28} steps on the average [KRS85].[4] It is possible that DES is pure, but not closed. (Of course, if DES were closed, then DES would also be pure.) Although there is no particular reason to suspect that DES is pure, it is unknown in the open literature if DES has this weakness.

The question "Is DES closed?" is a question about the order of the group generated by DES. A related and more detailed question—which we call the *small subgroup question*—is: "What is the order of the group generated by n given DES transformations?" Any set of DES transformations that generates a small group would suffer the weaknesses of closed ciphers. Specifically, any such set of transformations would be vulnerable to our known-plaintext attack against closed ciphers. In addition, multiple encryption (using either sequential multiple encryption or Tuchman's scheme) involving only transformations from such a set would be equivalent to single encryption from the set.[5] Finally, when used in output-feedback mode with feedback width 64 [FIS80], any transformation from such a set would be at greater risk to produce a key stream with short period.

[2] The Data Encryption Standard (DES) is a federal standard for the cryptographic protection of computer data, adopted in November 1976 by the United States National Bureau of Standards (NBS) [FIPS77,DaP84].

[3] See section 2.1 for a review of the definition of a pure cipher.

[4] To encrypt a message x under *Tuchman's scheme* is to compute $T_i T_j^{-1} T_k(x)$, where the keys i, j, and k are chosen independently [Tuc78,MeM82].

[5] To encrypt a message x using *sequential multiple encryption* is to compute $T_i T_j(x)$, where the keys i and j are chosen independently [MeH81].

Two of our tests address the small subgroup question for $n = 1, 2$.

To test DES for purity and other algebraic weaknesses, we examined the orbits of subsets of DES transformations on particular messages. Our method was to compute the orbits of single DES transformations and to apply our cycling closure test to subsets of two or more DES transformations. To carry out the tests we built special-purpose hardware and implemented a variation of the constant-space cycle-detection algorithm described by Sedgewick and Szymanski [SSY82]. We applied our tests both to randomly chosen transformations and to transformations with special properties (*e.g.* transformations represented by weak keys). The dominant theme of our tests was to determine if DES has algebraic properties different from those expected from a set of randomly selected permutations.

Since there is an overwhelming chance that even two randomly selected permutations will generate either the alternating group or the symmetric group [BoW77,Dix69], we did not expect to detect any pairs of DES transformations that generate small groups.

2 Background

2.1 Definitions and Notation

The Data Encryption Standard (DES) specifies a mapping $T : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$, where $\mathcal{K} = \{0,1\}^{56}$ is the *key space* and $\mathcal{M} = \{0,1\}^{64}$ is the *message space*. Each key $k \in \mathcal{K}$ represents a transformation $T_k = T(k, \cdot)$, which, by the definition of DES, permutes $\mathcal{M}$. DES is *endomorphic*: its message space and ciphertext space are the same set. It is unknown if DES is *faithful:* does every key represent a distinct permutation?

We shall use the following notations throughout the paper. Let $M = |\mathcal{M}| = 2^{64}$ be the *degree* of DES; let $K = |\mathcal{K}| = 2^{56}$ be the size of the key space; and let $\mathcal{T} = \bigcup\{T_k : k \in \mathcal{K}\}$ be the set of all DES transformations. In addition, for any transformation $T_k \in \mathcal{T}$, let T_k^{-1} denote the inverse of T_k.

Let I be the identity permutation on $\mathcal{M}$, and let $\mathcal{A}_\mathcal{M}$ and $\mathcal{S}_\mathcal{M}$ be, respectively, the *alternating group* and *symmetric group* on $\mathcal{M}$.[6] For any permutations g, h we denote the composition of g and h by $gh = g \circ h = g[h(\cdot)]$. For any permutations $g_1, g_2, \ldots, g_n$, let $\langle g_1, g_2, \ldots, g_n \rangle$ denote the group generated by $g_1, g_2, \ldots, g_n$. Of course, for any n DES transformations $T_1, T_2, \ldots, T_n$, it is true that $\langle T_1 \rangle \subseteq \langle T_1, T_2 \rangle \subseteq \langle T_1, T_2, \ldots, T_n \rangle \subseteq \langle \mathcal{T} \rangle$. Since each round of DES is an even permutation, it is also true that $\langle \mathcal{T} \rangle \subseteq \mathcal{A}_\mathcal{M}$.

For any subgroup $G \subseteq \mathcal{S}_\mathcal{M}$, for any $x \in \mathcal{M}$, the *G-orbit of* x is the set $G\text{-orbit}(x) = \{g(x) : g \in G\}$. For any permutation $g \in \mathcal{S}_\mathcal{M}$, may write $g\text{-orbit}(x)$ to denote the $\langle g \rangle$-orbit of x. If f is any function (not necessarily a permutation) and if $x \in \text{Domain}(f)$, we define the *f-closure of* x to be the set $f\text{-closure}(x) = \{f^i(x) : i \geq 0\}$. For any subgroup $G \subseteq \mathcal{S}_\mathcal{M}$, the *order of* G is the number of elements in G. For any $g \in \mathcal{S}_\mathcal{M}$, the *order of* g is the order of $\langle g \rangle$.

A cryptosystem is *closed* if and only if its set of encryption transformations is closed under functional composition, *i.e.* DES is closed if and only if for all keys $i, j \in \mathcal{K}$ there exists a key $k \in \mathcal{K}$ such that $T_i T_j = T_k$.[7] Since every finite cancellation semigroup is a group, DES is closed if and only if $\mathcal{T}$ forms a group under functional composition.

[6] See [Car56], [Rot78], or [Wie64] for a review of basic concepts in permutation group theory.

[7] Note that we are using the term *closed cipher* to refer to what Shannon called an *idempotent cipher* [Sha49]. Shannon defined a closed cipher to be any cryptosystem with the property that each cryptographic transformation is surjective.

Shannon's notion of a pure cipher generalizes the idea of closure to non-endomorphic cryptosystems [Sha49]. DES is *pure* if and only if, for every keys $i, j, k \in \mathcal{K}$, there exists a key $l \in \mathcal{K}$ such that $T_i T_j^{-1} T_k = T_l$.[8] It is easy to see that DES is pure if and only if *for every* $T_0 \in \mathcal{T}$ the set $T_0^{-1}\mathcal{T}$ is closed. Moreover, $T_0^{-1}\mathcal{T}$ is closed *for every* $T_0 \in \mathcal{T}$ if and only if $T_0^{-1}\mathcal{T}$ is closed *for some* $T_0 \in \mathcal{T}$. Every closed cryptosystem is pure, but not every endomorphic pure cryptosystem is closed.

Finally, for any any string $s \in \{0,1\}^*$, let $\overline{s}$ denote the bitwise complement of s.

2.2 Previous Cycling Studies on DES

To the best of our knowledge, the small subgroup question for two or more DES transformations had not been previously investigated in the open literature. A few researchers have, however, studied the pseudo-random key streams produced by DES in output-feedback mode [FIS80]. Whenever the feedback width is 64 bits, each such key stream describes the orbit of a DES transformation on some initial message. In a series of software experiments, Gait computed the key stream produced by DES in output-feedback mode to at most $10^6 \approx 2^{20}$ places. He found no cycles for nonweak keys [Gai77]. Gait did not state what feedback width he used. Davies and Price [DaP82,DaP82a] and Jueneman [Jue82] studied mathematically the cycle structure of the key stream produced in output-feedback mode, but did not report performing any experiments on DES. Davies and Price did run a series of experiments on random permutations on $\{0,1\}^8$ [DaP82a]. Finally, in a series of experiments, Hellman and Reyneri investigated the cycle structure of mappings induced by DES on the key space [HeR82]. None of these studies answered the question, "Is DES pure?"

2.3 Review of Cycling Closure Test

The cycling closure test is a statistical test that explores one aspect of the algebraic structure of any finite, deterministic cryptosystem. It works by taking a pseudo-random walk in the message space for a specified number of steps or until a cycle is detected. For each step of the pseudo-random walk, the previous ciphertext is encrypted under a key chosen by a pseudo-random function of the previous ciphertext. Results of the test are asymmetrical: long walks are overwhelming evidence that the set of permutations is not a group; short walks are strong evidence that the set of permutations has a structure different from that expected from a set of randomly chosen permutations [KRS85].

When applied to DES and given an initial message x_0, the cycling closure test computes the ψ_ρ-closure of x_0, where the function $\psi_\rho : \mathcal{M} \to \mathcal{M}$ is defined by $\psi_\rho(x) = T_{\rho(x)}(x)$ whenever $x \in \mathcal{M}$, and $\rho : \mathcal{M} \to \mathcal{K}$ is a deterministic pseudo-random function. If ρ is "random," then ψ_ρ acts like a random function on the $\langle\mathcal{T}\rangle$-orbit of x_0. The expected length of the ψ_ρ-closure computed by the test is about the square root of the length of the $\langle\mathcal{T}\rangle$-orbit of x_0.

When applied to a subset $S \subseteq \mathcal{T}$ of two or more DES transformations, the cycling closure test computes the ψ_ρ-closure of x_0, where $\rho : \mathcal{M} \to H$ and $H \subseteq \mathcal{K}$ is a set of keys that represents S.

If DES acts like a set of randomly chosen permutations, then we would expect $\langle\mathcal{T}\rangle$-orbit$(x_0) = \mathcal{M}$, in which case we would expect $|\psi_\rho\text{-closure}(x_0)| \approx \sqrt{M} = 2^{32}$. However, if DES were closed, then $|\langle\mathcal{T}\rangle\text{-orbit}(x_0)| \leq K$, in which case we would expect $|\psi_\rho\text{-closure}(x_0)| \leq \sqrt{K} = 2^{28}$.

[8] Shannon also required each transformation of a pure cipher to be equally likely.

The cycling closure test collects evidence which can be used to compute a measure of our relative degree of belief in the following two competing hypotheses:

- H_G = "DES is a group."
- H_R = "Each DES transformation was chosen independently with uniform probability from the symmetric group on $\mathcal{M}$."

Let E be the evidence that a trial of the cycling closure test ran for r steps without detecting a cycle. As explained in [KRS85], this evidence can be interpreted by computing the conditional probabilities $p_G = P(E \mid H_G)$ and $p_R = P(E \mid H_R)$, where

$$p_G \approx e^{-r^2/2K} \text{ and } p_R \approx e^{-r^2/2M}. \tag{1}$$

In light of the evidence E, a Bayesian would update her initial odds in favor of H_G over H_R by a factor of p_G/p_R.

2.4 Special-Purpose Hardware

We carried out each experiment using special-purpose hardware which we had originally built to test DES for closure. The main feature of our hardware is that it can compute a sequence of 2^{32} DES encryptions per day, where at each step the previous ciphertext is encrypted under a key that depends on the previous ciphertext. Our hardware consists of a custom wire-wrap board that plugs into an IBM personal computer. The board contains one AMD Z8068 DES chip and a 7.1 MHz finite state controller. By modifying the microcode of the board's finite-state controller, we adapted the board to carry out each of the five algebraic tests. (See [KRS85] for a more detailed description of our special-purpose hardware.[9])

3 Cycling Experiments on DES

This section briefly describes the four additional cycling tests that we performed on DES. We call these tests the *purity test*, *orbit test*, *small subgroup test*, *closure test*, and *extended message space closure test*. A sixth *reduced message space test* is also described.

3.1 Purity Test

Pick any transformation $T_0 \in \mathcal{T}$ and apply the cycling closure test to the set $T_0^{-1}\mathcal{T}$. (See section 2.3 for a review of the cycling closure test.)

3.2 Orbit Test

Given any key k and any message x_0, compute $x_i = T_k^i(x_0)$, $i = 1, 2, \ldots$ for a specified number of steps or until a cycle is detected.

The period of this sequence is the length of T_k-orbit(x_0). In other words, if we consider the permutation T_k as a product of disjoint cycles, then the period of the sequence is simply the

[9] Schematic diagrams of our hardware will be included in a revised version of this paper, to be available from the authors some time in the future.

length of the cycle that contains x_0. If this test is run for r steps without detecting a cycle, then r is a lower bound on order(T_k) and hence on order($\langle \mathcal{T} \rangle$).

For a randomly chosen permutation on M, for each $1 \leq l \leq M$, the probability that x_0 lies in a cycle of length exactly l is $1/M$ [Har59,PuW68] ([Knu69], exercise 3.1.12). Hence, the expected cycle-length of the longest cycle of a randomly chosen permutation on n letters is about $0.624n$ [ShL66] (for DES, this is about 2^{63}). For a randomly chosen permutation on M, the chance that we fall into a cycle of length 2^{36} or less is about $2^{-(63-36)} = 2^{-27}$.

Although we do not do so in this preliminary abstract, it is possible to interpret results of the orbit test to obtain statistical lower bounds on the order of the group generated by DES. Such analysis depends on the structure of the group. For example, the orbit test behaves differently on cyclic groups than on symmetric groups. Consequently, it is useful to combine the orbit test with other algebraic tests, including tests for faithfulness, commutativity, solvability at various levels, and nilpotence at various classes.

3.3 Small Subgroup Test

Given two distinct keys $i, j \in K$ and any message x_0, apply the cycling closure test to the set $\{T_i, T_j\}$ to obtain a statistical lower bound on the length of the $\langle T_i, T_j \rangle$-orbit of x_0.

In the orbit and small group tests, it would be interesting to examine both randomly chosen transformations and certain "special" transformations. For example, it would be interesting to explore weak keys, semi-weak keys, light keys (keys with a low density of ones), heavy keys (keys with a high density of ones), and pairs of related keys (*e.g.* keys that differ in one bit and keys that are complements of each other).

3.4 Extended Message Space Closure Tests

For any experiment that uses the cycling closure test, perform the cycling closure test with an extended message space space that consists of the Cartesian product M^l of the original message space, for some small integer l.[10]

The closure test works by computing a statistical lower bound on the length of $\langle \mathcal{T} \rangle$-orbit($x_0$), which, in turn, yields a lower bound on the order of $\langle \mathcal{T} \rangle$. Limits on the lower bounds achievable by this test are imposed both by the number of steps the test is carried out and by the relative sizes of the message space and key space. For all $1 \leq r \leq \sqrt{M}$, if the test is run for r steps without detecting a cycle, then with high probability order($\langle \mathcal{T} \rangle$) $\geq r^2$. To use the cycling closure test to obtain statistical lower bounds on order($\langle \mathcal{T} \rangle$) greater than 2^{64}, it is necessary to perform an extended message test with $l > 1$.

3.5 Reduced Message Space Tests

Perform each of the above tests on a modified version of DES in which the message space is reduced in size. Specifically, consider DES-derived functions $\phi_k : M_r \to M_r$ on the reduced message space $M_r = \{0,1\}^r$, where r is some small integer (say, $r = 8$) and ϕ_k is defined as follows. For each key $k \in K$, define ϕ_k by $\phi_k = \pi_2 T_k \pi_1$, where $\pi_1 : M_r \to M$ is an injection and $\pi_2 : M \to M_r$ is a projection. (For example, π_1 might fix the first 56 DES input bits to 0, and π_2 might take only the last 8 DES output bits.)

[10] In the extended message space closure test, the pseudo-random function ρ maps M^l into K.

No.	Experiment	Leader length	Cycle length	p_G	p_R
1	Closure	$\approx 2^{25}$	$\approx 2^{33}$	$\leq 10^{-193}$	≥ 0.17
2	Closure	$\approx 2^{30}$	$\approx 2^{33}$	$\leq 10^{-264}$	≥ 0.09
3	Closure	$\approx 2^{31}$	$\approx 2^{30.5}$	$\leq 10^{-41}$	≥ 0.68
4	Extended closure	(no cycle in 2^{34} steps)		$\leq 10^{-889}$	$\geq 1 - 10^{-18}$
5	Purity	$\approx 2^{31.5}$	$\approx 2^{30}$	$\leq 10^{-61}$	≥ 0.57
6	Purity	$\approx 2^{30}$	$\approx 2^{32}$	$\leq 10^{-94}$	≥ 0.42
7	Small subgroup	0	$\approx 2^{33}$	*	$\leq 10^{-9}$
8	Orbit	(no cycle in 2^{36} steps)		*	$\geq 1 - 10^{-8}$

* Depends on hypothesized group structure.

Table 1: Summary of DES experiments, May–August, 1985. (The numbers p_G and p_R are the conditional probabilities of the experimental evidence under the hypotheses "DES is closed (pure)" and "Each DES transformation was drawn at random from the symmetric group on $\mathcal{M}$" respectively.)

Studying reduced message space versions of DES is useful for two reasons. First, it is one way to look for structures that may be present on subsets of the message space. Second, by sufficiently restricting the message space, it is possible to write down a complete description of the action of particular transformations on the reduced message space.

4 Experimental Results and Conclusions

This section summarizes our experimental results and discusses two interesting structural findings.

4.1 Summary of Experimental Results

During May to August 1985, we performed eight cycling experiments covering five different algebraic tests. Specifically, we performed three closure tests, one extended message space closure test, two purity tests, one small subgroup test using two of the weak keys, and one orbit test.[11] These experiments gathered overwhelming statistical evidence that DES is neither pure nor closed and that the size of the group generated by DES is at least 2^{68}. Table 1 summarizes our experimental results.

As one test of correctness, we ran a software implementation of the cycling closure test for 30,000 steps. The software and hardware implementations agreed on all values. As a second test of correctness, we repeated experiments 1 and 2 and obtained identical results. We invite the interested reader to verify our results using the detailed experimental data found in appendix A.

In experiment 7, we applied the small subgroup test to the transformations represented by the two weak keys that consist respectively of all zeros and all ones. Since each of the weak transformations is self inverse, we implemented this test as an orbit test using the composition of the weak transformations. This experiment produced a short cycle of about 2^{33} steps, which would be unusual (probability less than 10^{-9}) if the tested permutation were chosen at random from $S_{\mathcal{M}}$.

[11] We also performed one trial of a reduced message space closure test that detected no algebraic weaknesses.

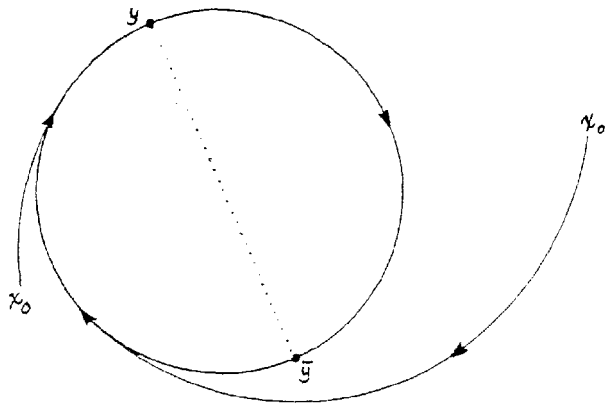

Figure 1: Results of experiments 1 and 2. Starting at different initial messages, both pseudo-random walks entered the same cycle. Every message on the cycle is the bitwise complement of the corresponding message halfway around the cycle.

4.2 Two Structural Findings

Although most of our experimental results are consistent with the hypothesis that DES acts like a set of randomly chosen permutations, three experiments did yield interesting regularities. One regularity is a result of the well-known complementation property;[12] the other involves a newly discovered property of the weak keys. We will now explain these structural findings.

4.2.1 Complementation and Drainage Properties

In the first two experiments, we performed two independent trials of the cycling closure test. Each of these experiments used the "identity" next key function—the function $\rho: \mathcal{M} \rightarrow \mathcal{K}$ that removes each of the eight parity bits. These two experiments produced two interesting findings. First, each of the pseudo-random walks drained into the same cycle. Second, each point on the cycle was the bitwise complement of the corresponding point exactly halfway around the cycle. Figure 1 illustrates these findings.

The first finding is explained by the fact that, for the graph of a randomly chosen function, most points on the graph will probably drain into the same cycle. See [HeR82] for one analysis of this phenomenon.

The second finding is a consequence of DES's complementation property and the fact that the identity next key function also has a complementation property (for all messages x, $\rho(\overline{x}) = \overline{\rho(x)}$). The cycling closure test computes a pseudo-random walk $x_0, x_1, \ldots$, where $x_{i+1} = T_{\rho(x_i)}(x_i)$, for $i \geq 1$. If $x_i = \overline{x_j}$ for any $i > j$, then it would follow that

$$x_{i+1} = T_{\rho(x_i)}(x_i) = T_{\rho(\overline{x_j})}(\overline{x_j}) = T_{\overline{\rho(x_j)}}(\overline{x_j}) = \overline{T_{\rho(x_j)}(x_j)} = \overline{x_{j+1}}\,. \tag{2}$$

Therefore, by induction, $x_{i+h} = \overline{x_{j+h}}$ for all $h \geq 0$. This situation arises whenever some $x_i = \overline{x_j}$ before any $x_i = x_j$ with $i > j$, which will happen for about half of all initial messages.

[12] For every key k and every message x, $T_k(x) = \overline{T_{\overline{k}}(\overline{x})}$ [DaP84].

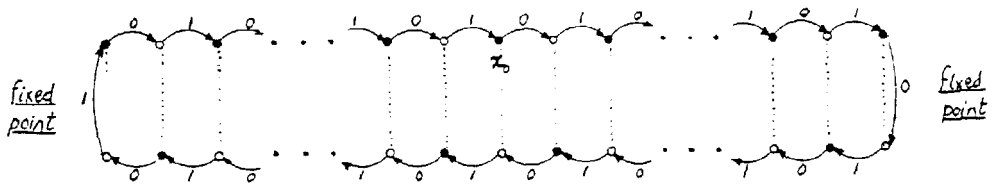

Figure 2: Results of experiment 7. (Filled circles denote the messages x_i on the $T_{1\ldots1}T_{0\ldots0}$-orbit of an initial message x_0. Unfilled circles denote intermediate values $T_{0\ldots0}(x_i)$. Dotted lines link identical messages.)

4.2.2 Fixed Points of the Weak Keys

In experiment 7, we computed the orbit of a message under the composition of the two weak keys that consist respectively of all zeros and all ones. Although each weak key is self-inverse, we did not expect the composition to produce short orbits. Much to our surprise, we detected a cycle of length less than 2^{33}. We presented this finding at the Crypto 85 conference and sought a simple explanation.

After some thought, Don Coppersmith suggested that we had encountered fixed points of the weak keys, *i.e.*, messages x for which $T_{1\ldots1}(x) = x$ or $T_{0\ldots0}(x) = x$. Since each weak key yields 16 identical round keys, for each weak key, a fixed point results whenever DES's L and R registers agree after eight rounds. Since the middle L and R registers are equal with probability about $1/2^{32}$, there should be about 2^{32} fixed points for each of the four weak keys. Hence, by 2^{33} steps, it was likely that we had encountered a fixed point. Figure 2 illustrates the effect of the fixed points on the walk in the message space and explains why a cycle resulted.

After the conference, we found the fixed points and thus confirmed Coppersmith's hypothesis (see appendix). To the best of our knowledge, these fixed points are the first published in the open literature. These fixed points further illustrate the deficiencies of the weak keys.

Coppersmith also suggested that the algebraic structure detected in experiment 7 can be used to prove strong lower bounds on the size of the group generated by DES. Experiment 7 computed the length, l, of the g-orbit of x_0, where $g = T_{1\ldots1}T_{0\ldots0}$ is composition of two DES transformations and x_0 is the initial message. Since l divides the order of g, it follows that l divides the order of the group generated by DES. Therefore, if experiment 7 were repeated r times with different initial messages, and if these experiments yielded orbit lengths $l_1, l_2, \ldots, l_r$, then $\mathrm{lcm}(l_1, l_2, \ldots, l_r)$ would be a lower bound on the order of the group generated by DES. We have not yet extended our results in this direction.

Acknowledgments

We would like to thank several people who contributed to this paper. Leon Roisenberg helped out with the design and construction of our special-purpose hardware. As part of his bachelor's thesis, John Hinsdale wrote the C software used by our host IBM personal computer to carry out the cycle-detection algorithm. We are also grateful to László Babai, Don Coppersmith, and Gary Miller for helpful comments. In addition, we would like to thank the Functional Languages and Architectures Research Group of the MIT Laboratory for Computer Science for use of their

hardware laboratory during the construction and testing of our special-purpose hardware.

References

[Bet82] Beth, Thomas, *ed.*, *Cryptography, Proceedings of the Workshop on Cryptography, Burg Feuerstein, Germany, March 29–April 2, 1982*, Springer (Berlin, 1983).

[Bov80] Bovey, J. D., "An approximate probability distribution for the order of elements of the symmetric group," *Bull. London Math Society*, **12** (1980), 41–46.

[BoW77] Bovey, John; and Alan Williamson, "The probability of generating the symmetric group," *Bull. London Math Society*, **10** (1978), 91–96.

[Car56] Carmichael, Robert D., *Introduction to the Theory of Groups of Finite Order*, Dover (New York, 1956).

[CRS82] Chaum, David; Ronald L. Rivest; and Alan T. Sherman, *eds.*, *Advances in Cryptology: Proceedings of Crypto 82*, Plenum Press (New York, 1983).

[DaP84] Davies, Donald W.; and W. L. Price, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer*, John Wiley (Chichester, England, 1984).

[Dav82] Davies, Donald W., "Some regular properties of the DES," in [CRS82], 89–96.

[DaP82] Davies, Donald W.; and G. I. P. Parkin, "The average size of the key stream in output feedback mode," in [CRS82], 97–98.

[DaP82a] Davies, Donald W.; and G. I. P. Parkin, "The average size of the key stream in output feedback encipherment," in [Bet82], 263–279.

[Dix69] Dixon, John D., "The probability of generating the symmetric group," *Math Zentrum*, **110** (1969), 199–205.

[FIPS77] "Data Encryption Standard," National Bureau of Standards, Federal Information Processing Standards Publications No. 46 (January 15, 1977).

[FIS80] "DES modes of operations," Federal Information Standards Publication No. 81 (December 1980).

[Gai77] Gait, Jason, "A new nonlinear pseudorandom number generator," *IEEE Transactions on Software Engineering*, **SE-3** (September 1977), 359–363.

[Har59] Harris, Bernard, "Probability distributions related to random mappings," *Annals of Math. Statistics*, **31** (1959), 1045–1062.

[Hel76] Hellman, Martin E., *et al.*, "Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard," technical report SEL 76–042, Information Systems Laboratory, Stanford Univ. (November 1976).

[HeR82] Hellman, Martin E.; and Justin M. Reyneri, "Distribution of Drainage in the DES," in [CRS82] (1982), 129–131.

[Jue82] Jueneman, Robert R., "Analysis of certain aspects of output-feedback mode," in [CRS82] (1982), 99–127.

[KRS85] Kaliski, Burton S., Jr.; Ronald L. Rivest; and Alan T. Sherman, "Is the Data Encryption Standard a Group?" *Proceedings of Eurocrypt 85*, Springer, to appear.

[Knu69] Knuth, Donald E., *Seminumerical Algorithms* in *The Art of Computer Programming*, vol. 2, Addison-Wesley (1969).

[MeH81] Merkle, Ralph C.; and Martin E. Hellman, "On the security of multiple encryption," *CACM*, **24** (July 1981), 465–467.

[MeM82] Meyer, Carl H.; and Stephen M. Matyas, *Cryptology: A New Dimension in Computer Data Security*, John Wiley (New York, 1982).

[PuW68] Purdom, Paul W.; and J. H. Williams, "Cycle length in a random function," *Transactions of the American Mathematics Society*, **133** (1968), 547–551.

[Rot78] Rotman, Joseph J., *The Theory of Groups: An Introduction*, Allyn and Bacon (Boston, 1978).

[Sha49] Shannon, Claude E., "Communication theory of secrecy systems," *Bell System Technical Journal*, **28** (October 1949), 656–715.

[SSY82] Sedgewick, Robert; Thomas G. Szymanski; and Andrew C. Yao, "The complexity of finding cycles in periodic functions," *Siam Journal on Computing*, **11** (1982), 376–390.

[ShL66] Shepp, L. A.; and S. P. Lloyd, "Ordered cycle lengths in a random permutation," *Transactions of the American Mathematics Society*, (February 1966), 340–357.

[Tuc78] Tuchman, W. L., talk presented at National Computer Conference, (June 1978).

[Wie64] Wielandt, Helmut, *Finite Permutation Groups*, Academic Press (New York, 1964).

A Detailed Descriptions of Experiments

This appendix presents nine tables that describe in detail the cycling experiments we carried out during summer 1985. The first table defines the pseudo-random next key function used in several of the experiments. The remaining eight tables—one for each experiment—list all relevant experimental parameters together with important checkpoints encountered during the experiments.

A.1 Notation

In the body of the abstract, we defined the key space of DES to be the set $K = \{0,1\}^{56}$. Most DES implementations, however, nominally treat each key as a string of 64 bits, where every eighth key bit is a *parity bit* which is ignored. In this appendix, we too shall specify keys and messages as 64-bit strings, described in hexadecimal notation. To do this, it is convenient to introduce the DES function $\hat{T}: \hat{K} \times M \to M$ that operates on the nominal key space $\hat{K} = \{0,1\}^{64}$.

A.2 Next Key Functions

The cycling closure test depends on a function $\rho: M \to K$ to compute the next key from the current message. We will now describe the two particular *next key functions* that we used during our experiments. We will define each next key function in terms of its related function $\hat{\rho}: M \to \hat{K}$.

Each next key function operated in a byte-by-byte fashion using a byte substitution table (1 byte = 8 bits). For any $0 \le i \le 7$ and any $x \in M$, let $x^{(i)}$ denote the i^{th} byte of x. For each $0 \le i \le 7$, we computed $\hat{\rho}(x)^{(i)} = S(x^{(i)})$, for some byte substitution table $S: \{0,1\}^8 \to \{0,1\}^8$.

In experiments 1 and 2, we chose S to be the identity function. In the other cycling closure experiments, we used the byte substitution table given by table 2.[13] This table was designed so that each entry has odd parity and such that each entry appears exactly twice. The table was generated using the random number generator in the C library on our IBM PC.

For the experiments that used the extended message space M^2, we computed $\hat{\rho}(x)^{(i)} = S(x^{(2i)})$ using the substitution table given in table 2.

A.3 Selection of Experimental Parameters

We chose initial messages and keys in a variety of *ad hoc* ways. Some we selected in an obviously deterministic manner (*e.g.*, $x_0 =$ 0123456789ABCDEF). Others are related to the authors' social security numbers or other personal data. The rest we generated using DES and MACSYMA.

A.4 Detailed Experimental Results

Tables 3–10 list the detailed results of our cycling experiments.

[13] The substitution table is used as follows. To substitute any byte B, consider the representation of B as two hexadecimal digits. Select the table entry whose row is given by the first digit and whose column is given by the second digit.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00	3E	46	B6	26	AE	F8	2A	AE	CE	57	E6	98	07	5D	92	2C
10	FE	58	EF	CD	F7	76	2F	91	8F	2F	0E	D0	07	B0	73	51
20	20	5E	76	B3	86	9D	16	01	31	EF	D3	8F	D6	40	2A	F8
30	01	C7	C7	19	F7	31	A2	62	9E	B9	DA	D9	34	85	19	D9
40	61	A8	3D	B0	0E	79	C2	BC	52	04	37	FD	6E	85	FB	BA
50	DF	C8	6D	13	43	1C	0B	4A	89	83	E3	20	4F	A7	BA	3B
60	80	D0	67	EA	7F	A8	C8	43	79	6D	1A	4C	A7	CB	86	23
70	5B	02	C2	4C	58	38	FE	CE	B9	1C	15	A4	25	29	1A	15
80	C1	98	7F	4A	64	57	97	32	26	F2	E5	91	D6	E9	6B	F4
90	4F	80	67	DF	F1	BF	B3	B5	3E	E5	7A	EC	A1	B5	92	29
A0	10	DC	97	46	94	CB	49	6B	10	45	3B	F2	E6	FD	B6	BC
B0	40	0D	1F	AD	52	BF	62	23	61	49	E0	0D	08	CD	E3	C4
C0	68	1F	9E	E9	FB	7C	13	75	8A	89	04	5D	6E	DC	54	D5
D0	EA	F1	9D	F4	94	75	D3	70	8C	54	AB	2C	D5	02	98	7A
E0	3D	5B	25	8A	A1	38	8C	EC	70	9B	A4	45	64	51	AB	7C
F0	C1	AD	34	C4	E0	A2	68	83	16	08	DA	32	73	37	0B	5E

Table 2: Byte substitution table for pseudo-random next key function.

Experiment 1		$x_{i+1} = \hat{T}_{x_i}(x_i)$
i	x_i	*Note*
0	0123456789ABCDEF	
34,293,588	B0FDED3BD0DD918C	*end of leader*
34,293,589	AE5530A0E971B5E8	*start of cycle*
2,030,556,568	12B67D3796106D30	*quarter cycle*
4,026,819,547	51AACF5F168E4A17	*half cycle*
6,023,082,526	ED4982C869EF92CF	*three-quarters cycle*
8,019,345,504	A032CE0D3F436EFE	*end of cycle*
8,019,345,505	AE5530A0E971B5E8	*restart of cycle*

Table 3: Closure experiment with identity next key function. Cycle length 7,985,051,916 $\approx 2^{33}$; leader length 34,293,589 $\approx 2^{25}$.

Experiment 2		$x_{i+1} = \hat{T}_{x_i}(x_i)$
i	x_i	*Note*
0	12150285080020664	
1,389,523,413	48BB5C9F85CD285A	*end of leader*
1,389,523,414	AFF50E97653421BF	*start of cycle*
5,152,082,299	AE5530A0E971B5E8	*experiment 1 intersection*
9,374,575,329	FB0A1398E92D1473	*end of cycle*
9,374,575,330	AFF50E97653421BF	*restart of cycle*

Table 4: Closure experiment with identity next key function. Cycle length 7,985,051,916 $\approx 2^{33}$; leader length 1,389,523,414 $\approx 2^{30}$.

Experiment 3		$x_{i+1} = \tilde{T}_{\hat{p}(x_i)}(x_i)$
i	x_i	*Note*
0	6036222982B03104	
2,138,241,978	68955F4BF000A6E0	*end of leader*
2,138,241,979	C9DB8E7169CCF272	*start of cycle*
3,706,679,992	433B74E2CB18DDFD	*end of cycle*
3,706,679,993	C9DB8E7169CCF272	*restart of cycle*

Table 5: Closure experiment with pseudo-random next key function. Cycle length $1{,}568{,}438{,}014 \approx 2^{30.5}$; leader length $2{,}138{,}241{,}979 \approx 2^{31}$.

Experiment 4		$x_{i+1} = \tilde{T}_{\hat{p}(x_i)}(x_i), x_i \in M^2$
i	x_i	*Note*
0	4C957F303AC4D08B 63E15C9C7A398042	
4,294,967,296	2C173869EAF8804B 767469BB19B26D8A	2^{32} *iterations*
8,589,934,592	4349368A49700D3B 55FC02F8848BC64F	2^{33} *iterations*
12,884,901,888	55D1292F5D99B268 C30AB80FF3B03D08	$3 \cdot 2^{32}$ *iterations*
17,179,869,184	4A224C65B8A48DEB 00C7D0CA64C4B240	2^{34} *iterations*

Table 6: Extended closure experiment with pseudo-random next key function. No cycle detected in 2^{34} steps.

Experiment 5		$x_{i+1} = \tilde{T}_{\hat{k}}^{-1} \tilde{T}_{\hat{p}(x_i)}(x_i)$
i	x_i	*Note*
0	0123456789ABCDEF	
3,233,340,362	0EC45F7157BD8749	*end of leader*
3,233,340,363	EFE7B7112233DD88	*start of cycle*
4,531,729,424	C09DFA478C3849BE	*end of cycle*
4,531,729,425	EFE7B7112233DD88	*restart of cycle*

Table 7: Purity experiment with pseudo-random next key function. Cycle length $1{,}298{,}389{,}062 \approx 2^{30}$; leader length $3{,}233{,}340{,}363 \approx 2^{31.5}$. Key $\hat{k} =$ 97778E1BC3FD8E07.

Experiment 6		$x_{i+1} = \hat{T}_{\hat{k}}^{-1} \hat{T}_{\hat{\gamma}(x_i)}(x_i)$
i	x_i	*Note*
0	121502850B020664	
1,366,287,307	E43D6EF9351DDB4A	*end of leader*
1,366,287,308	75C6C23C21EA50DA	*start of cycle*
5,584,675,814	FDBE1ECDF38BF3E5	*end of cycle*
5,585,675,815	75C6C23C21EA50DA	*restart of cycle*

Table 8: Purity experiments with pseudo-random next key function. Cycle length $4{,}218{,}388{,}507 \approx 2^{32}$; leader length $1{,}366{,}287{,}308 \approx 2^{30}$. Key $\hat{k} =$ 4D3FD0FED9A4FA9B.

Experiment 7		$x_{i+1} = \hat{T}_{1\ldots1}(\hat{T}_{0\ldots0}(x_i))$
i	x_i	*Note*
0	0123456789ABCDEF	*start of cycle*
2,227,161,945	654B672D3DBC73AB	0...0 *fixed point*
4,454,323,890	293FD4F2C13DD94F	*"hidden crossing"*
5,890,012,565	3CC5B06ADEFD30A0	1...1 *fixed point*
7,325,701,239	0123456789ABCDEF	*restart of cycle*

Table 9: Small subgroup experiment using weak keys. Cycle length $7{,}325{,}701{,}239 \approx 2^{33}$; leader length 0.

i	x_i	*Note*
17,179,869,184	B98C3A67CD6F8267	2^{34} *iterations*
34,359,738,368	632509BC9F57DF8A	2^{35} *iterations*
51,539,607,552	ED4B06ABBF5515FB	$3 \cdot 2^{34}$ *iterations*
68,719,476,736	2C84263510AEAD34	2^{36} *iterations*

Table 10: Orbit experiment. No cycle detected in 2^{36} steps. Key $\hat{k} =$ 116E0B8278AEC431.