ON THE DESIGN OF S-BOXES

A. F. Webster and S. E. Tavares
Department of Electrical Engineering
Queen's University
Kingston, Ont.
Canada

The ideas of completeness and the avalanche effect were first introduced by Kam and Davida [1] and Feistel [2], respectively. If a cryptographic transformation is complete, then each ciphertext bit must depend on all of the plaintext bits. Thus, if it were possible to find the simplest Boolean expression for each ciphertext bit in terms of the plaintext bits, each of those expressions would have to contain all of the plaintext bits if the function was complete. Alternatively, if there is at least one pair of n-bit plaintext vectors X and X_i that differ only in bit i, and f(X) and $f(X_i)$ differ at least in bit j for all

$$\{(i,j) \mid 1 \leq i,j \leq n\}$$

then the function f must be complete.

For a given transformation to exhibit the avalanche effect, an average of one half of the output bits should change whenever a single input bit is complemented. In order to determine whether a given m × n (m input bits and n output bits) function f satisfies this requirement, the 2^m plaintext vectors must be divided into 2^{m-1} pairs, X and X_i, such that X and X_i differ only in bit i. Then the 2^{m-1} exclusive-or sums

$$V_i = f(X) \oplus f(X_i)$$

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 523-534, 1986.

must be calculated. These exclusive-or sums will be referred to as avalanche vectors, each of which contains n bits, or avalanche variables.

If this procedure is repeated for all i such that $1 \leq i \leq m$, and one half of the avalanche variables are equal to 1 for each i, then the function f has a good avalanche effect. Of course this method can be pursued only if m is fairly small; otherwise, the number of plaintext vectors becomes too large. If that is the case then the best that can be done is to take a random sample of plaintext vectors X, and for each value of i calculate all the avalanche vectors V_i. If approximately one half the resulting avalanche variables are equal to 1 for all values of i, then we can conclude that the function has a good avalanche effect.

THE STRICT AVALANCHE CRITERION AND THE INDEPENDENCE OF AVALANCHE VARIABLES

The concepts of completeness and the avalanche effect can be combined to define a new property which we shall call the strict avalanche criterion. If a cryptographic function is to satisfy the strict avalanche criterion, then each output bit should change with a probability of one half whenever a single input bit is complemented. A more precise definition of the criterion is as follows. Consider X and X_i, two n-bit, binary plaintext vectors, such that X and X_i differ only in bit i, $1 \leq i \leq n$. Let

$$V_i = Y \oplus Y_i$$

where $Y = f(X)$, $Y_i = f(X_i)$ and f is the cryptographic transformation under consideration. If f is to meet the strict avalanche criterion, the probability that each bit in V_i is equal to 1 should be one half over the set of all possible plaintext vectors X and X_i. This should be true for all values of i. Again, unless n is small it would be an immense task to follow this procedure for all possible vector pairs X and X_i.

An alternate method which could be used to ascertain whether a given cryptographic transformation, f, satisfies the strict avalanche criterion would be to construct a dependence matrix. First an n-bit, random plaintext vector X is generated and its corresponding m-bit ciphertext, Y = f(X), is obtained (n and m will be equal if f is an invertible transformation and there is no data expansion). Then the set of n vectors

$$(X_1, X_2, \ldots, X_n)$$

is formed such that X and X_j differ only in bit j. The ciphertext vectors

$$(Y_1, Y_2, \ldots, Y_n)$$

are then found where $Y_j = f(X_j)$, and they are used to obtain the set of m-bit binary avalanche vectors

$$(V_1, V_2, \ldots, V_n)$$

such that $V_j = Y \oplus Y_j$. This procedure is illustrated in Figure 1.

The value of bit i in V_j (either a 1 or a 0) is added to element $a_{i,j}$ in the m × n dependence matrix A. This procedure is repeated for a large number, r, of randomly generated plaintext vectors X, and each element in A is divided by r. Then each $a_{i,j}$ gives the strength of the relationship between plaintext bit j and ciphertext bit i. A value of 1 indicates that whenever bit j is complemented in the plaintext then the ciphertext bit i will also change its value, while a value of 0 indicates that the ciphertext bit is completely independent of the plaintext bit. If all elements in the matrix have a nonzero value then the cryptographic transformation is complete, and if it is to satisfy the strict avalanche criterion, every element must have a value close to one half. Therefore, completeness is a necessary condition if the strict avalanche criterion is to be met.

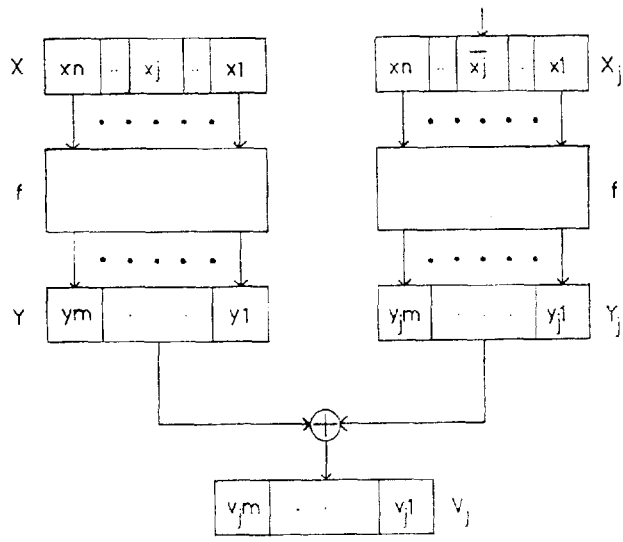

Figure 1. Part of the method for testing to see if a transformation satisfies the strict avalanche criterion: Input bit j is complemented giving V_j. Each bit i, $1 \leq i \leq m$, in V_j is added to element $a_{i,j}$ in the dependence matrix.

A second property which would seem desirable for any cryptographic transformation is that, for a given set of avalanche vectors generated by the complementing of a single plaintext bit, all the avalanche variables should be pairwise independent. In order to measure the degree of independence between a pair of avalanche variables, we can calculate their correlation coefficient. For two variables A and B

$$\rho\{A, B\} = \frac{\text{cov}\{A, B\}}{\sigma\{A\}\,\sigma\{B\}} \qquad [3, \text{p.378}]$$

where

$\rho\{A, B\}$ = correlation coefficient of A and B

$cov\{A, B\}$ = covariance of A and B

$= E\{AB\} - E\{A\} \times E\{B\}$

$\sigma^2\{A\} = E\{A^2\} - (E\{A\})^2$

For the case of binary variables, it can be shown that a correlation coefficient of 0 means that the variables are independent. In addition, the variables will always be identical if the correlation coefficient equals 1, and a value of -1 means that they will always be complements of one another [4].

If either the strict avalanche criterion or the avalanche variable independence requirement is not satisfied, then a cryptanalyst can gain some information about the statistical properties of the function, which he could conceivably use to his advantage in an attack on the system.

PERFECT S-BOXES

Now that these two new criteria have been presented, it would seem desirable to discover how to produce cryptographic transformations which satisfy both conditions. One additional condition that will be imposed on such transformations is that they be invertible. This means that there must be a one-to-one correspondence between plaintext and ciphertext vectors.

If there are n input/output bits for a given function, there are $(2^n)!$ possible invertible transformations. This means that there will be approximately 2×10^{13} such functions for a four-bit system. Therefore, the search will be limited to 4 × 4 (four input/four output bit) substitution boxes (S-boxes).

The initial step is to find all the potentially invertible 4 × 1 functions that satisfy the strict avalanche criterion, which will be combined four at a time to produce 4 × 4 substitution boxes. A potentially invertible function returns a value of 1 for one half of the possible input vectors and a value of 0 for the other half. It is a necessary, but not sufficient, condition if the S-boxes formed from the single output bit functions are to be invertible. The 12,870 potentially invertible, 4 × 1 functions were tested, and it was found that while 12,618 of them were complete, only 1368 satisfied the strict avalanche criterion [4].

These 1368 functions can be divided into 9 equivalence classes or "families". Each family is closed under the following operations:

1. Complementing one or more of the input bits
2. Permuting the input bits
3. Complementing the output bit

Potential invertibility and adherence to the strict avalanche criterion are preserved over these operations.

The simplest procedure to follow in constructing the substitution boxes would be to randomly select potentially invertible, single output bit functions from the list of those that satisfy the strict avalanche criterion. First, these substitution boxes are tested to see if they are invertible. If they satisfy that requirement, they are then examined to see if, when each input bit is complemented, the resulting avalanche variables are pairwise independent. An S-box that displays both of these properties will be referred to as a "perfect" substitution box.

When the method of random selection of single output bit functions was followed, the probability of the resulting 4 × 4 S-boxes being invertible was only 1.2×10^{-3}, and only one S-box in 7.1×10^{5} was perfect [4]. During this search,

the families of single output bit functions which formed perfect S-boxes were noted. In an attempt to reduce the amount of effort required to produce perfect S-boxes, the families from which the 4 x 1 functions were selected were fixed so that only combinations which had produced perfect S-boxes in the initial search were used. This increased the frequency of occurence of perfect S-boxes by about a factor of one thousand. Several other approaches were tried which involved relaxing one or both of the strict avalanche criterion and the avalanche variable independence requirement, but none proved to be as good as choosing the single output bit functions from fixed family combinations.

In the process of building these S-boxes, it was discovered that if an S-box is complete, or even perfect, its inverse function may not be complete. This could become important if these inverse functions are used in the decryption process, for it would be desirable for any changes in the ciphertext to affect all bits in the plaintext in a random fashion, especially if there is not much redundancy in the original plaintext. Complete cryptographic transformations with inverses which are complete are described as being two-way complete, and if the inverse is not complete the transformation is said to be only one-way complete.

A COMPLETE S-P NETWORK

Kam and Davida [1] presented a method whereby an entire S-P network could be guaranteed to be complete if all the substitution boxes used in the procedure were complete. This entailed using specially designed bit permutations between the substitution layers. The networks can be of any size as long as

$$n = k^g$$

where

n = the number of input/output bits for the entire network

k = the number of input/output bits for each S-box

g = the number of substitution-permutation stages

Since completeness is a prerequisite if the strict avalanche criterion is to be met, we thought that perhaps by using perfect S-boxes in the system we could come up with a "perfect" system. A complete S-P network with n = 64, k = 4 and g = 3 was implemented. Unfortunately, it turned out that each output bit changed with a probability of only one eighth when a single input bit was complemented. In fact, it can be shown that the probability of an output bit changing will always be 2^{-g}. This was termed avalanche damping. The same test was run with complete S-boxes of the type that Kam and Davida suggested in their paper instead of perfect S-boxes. The mean value of elements in the dependence matrix was slightly higher at 0.19, but their variance was over one hundred times greater than that calculated when the perfect S-boxes were used [4]. In fact, some elements had values as low as 0.01, which represents a significant shortcoming in the system.

This test was repeated for S-P networks with perfect S-boxes and random bit permutations. A plot of the mean and variance of the elements in the dependence matrix is shown in Figure 2. After three rounds, the performance is poorer than that for the complete S-P network, but after about 12 rounds the strict avalanche criterion is satisfied. This result suggests that with the addition of several S-P stages with complete or perfect S-boxes and random bit permutations, a complete S-P network could still be guaranteed to be complete and would probably satisfy the strict avalanche criterion.

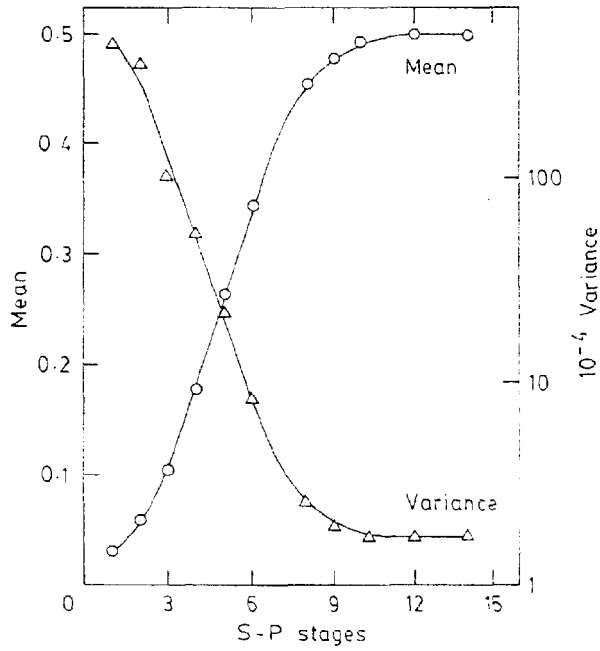

Figure 2. Mean and variance of elements in the dependence matrix for an S-P network vs. number of substitution-permutation stages: All the substitution boxes in this network were perfect, and the bit permutations were generated randomly. It is evident that the strict avalanche criterion is satisfied after approximately 12 S-P stages.

DES

The Data Encryption Standard (DES) has been a federal standard in the United States since 1977. DES employs substitutions and permutations, but the algorithm is much more complex than the one for the complete S-P network [5].

It can be shown that the DES algorithm is invertible [3, p.240]. Since the dependence matrix could, in theory, be different for every key, we cannot state that DES is always a "perfect" system. However, the results shown in Figure

3 for the key (FF . . . FF) indicate that in that case the strict avalanche criterion is satisfied. In addition, in a sample of 30 correlation coefficients picked at random, the highest absolute value found was 4.88×10^{-2}. This suggests that there is very little correlation between avalanche variables. Similar results were obtained using several other key values. Thus, we can conclude that DES is a "perfect" encryption algorithm, at least for the key values that were tested.

Since the S-boxes are the only nonlinear portion of the DES algorithm, their characteristics have a significant effect on the strength of the entire system. The S-boxes are not invertible, but due to the way in which they are employed in the algorithm, this does not pose a problem for decryption. Nor do they satisfy the strict avalanche criterion. For the entire set of 8 S-boxes, the probability that a particular output bit will change when a single input bit is complemented ranges from 0.43 to 0.93.

The correlation coefficients between pairs of avalanche variables for the DES S-boxes were also calculated. While most of them had absolute values of less than 0.5, it was found that when input bit 1 (the least significant bit in the input) was complemented, the correlation coefficients between bits 1 and 2 and between bits 3 and 4 in the output of S_4 were equal to -1. This is equivalent to the discovery made by Hellman et al. [6] that the exclusive-or sums of the output bits, $y1 \oplus y2$ and $y3 \oplus y4$, of S_4 are complemented whenever input bit x1 changes its value. It can also be shown that both of these results can be derived from another one of their findings

$$S_4(X \oplus 000001) = (2,1)(3,4)\ S_4(X) \oplus (x1, \overline{x1}, \overline{x1}, x1)$$

where (2,1)(3,4) means that the first and second bits as well as the third and fourth bits of the following vector are interchanged.

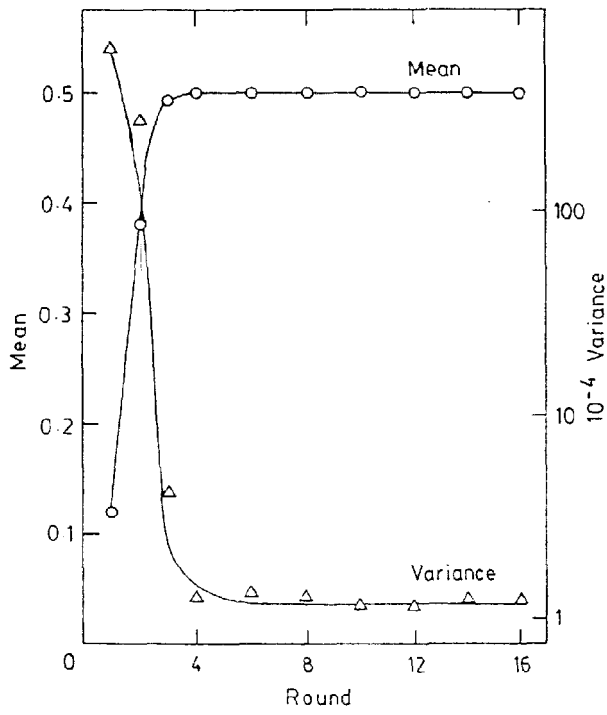

Figure 3. Mean and variance of DES dependence matrix vs. number of encryption rounds: These values of mean and variance are only for elements in one quarter of the dependence matrix, but Meyer [7] shows that these results will propagate through the rest of the matrix within two rounds. The strict avalanche criterion is satisfied after four rounds for this portion of the matrix; therefore, it will take six rounds before the full system will meet the requirement.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the financial support provided by the Natural Sciences and Engineering Research Council.

REFERENCES

[1] Kam, J.B., and Davida, G.I.: Structured Design of Substitution-Permutation Encryption Networks. IEEE Transactions on Computers, Vol. 28, No. 10, 747 (1979)

[2] Feistel, H.: Cryptography and Computer Privacy. Scientific American, Vol. 228, No. 5, 15 (1973)

[3] Konheim, A.G.: Cryptography: a Primer. John Wiley and Sons, New York (1981)

[4] Webster, A.F.: Plaintext/Ciphertext Bit Dependencies in Cryptographic Algorithms. M.Sc. thesis, Queen's University at Kingston (1985)

[5] National Bureau of Standards: Data Encryption Standard. FIPS Publication 46, Washington, D.C. (1977)

[6] Hellman, M.E., Merkle, R., Schroeppel, R., Washington, L., Diffie, W., Pohlig, S., and Schweitzer, P.: Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption Standard. SEL 76-042, Stanford University (1976)

[7] Meyer, C.H.: Ciphertext/Plaintext and Ciphertext/Key Dependence vs Number of Rounds for the Data Encryption Standard. 1978 National Computer Conference, p.1119. AFIPS Press, Montvale, New Jersey (1978)