Modelling Avalanche in DES-Like Ciphers

Howard M. Heys
Electrical Engineering
Memorial University of Newfoundland
St.John's, Newfoundland, Canada A1B 3X5
Email: howard@engr.mun.ca

Abstract: In this paper, we examine the avalanche characteristics of private-key block ciphers constructed using a DES-like architecture. Avalanche is a desirable cryptographic property that is necessary to ensure that a small difference between two plaintexts results in a seemingly random difference between the two corresponding ciphertexts. In order to examine the behaviour of DES-like ciphers in relation to the avalanche property, a model of the cipher is developed which allows us to analyze the avalanche characteristics of the cipher for different cipher parameter values. In particular, the results suggest that large, symmetric S-boxes which satisfy the guaranteed avalanche property are effective in combining efficiency and good avalanche characteristics of the cipher.

I. Introduction

Private-key block ciphers are typically implemented as a product cipher, using a number of rounds of substitutions and linear transformations. One such class of ciphers, introduced in [1] and referred to as DES-like or Feistel ciphers, uses the general structure of the Data Encryption Standard (DES) [2].

The concept of avalanche in block ciphers was informally introduced by Feistel [3] and Feistel, Notz, and Smith [1], as the property of a small number of bit changes in the plaintext input leading to an "avalanche" of changes in subsequent rounds resulting in a large number of ciphertext bit changes. More precisely, in our analysis, we consider the following definition of the avalanche criterion [4]:

Definition 1 : A cipher is said to satisfy the *avalanche criterion* if, for all keys, on average, half of the ciphertext bits change when one plaintext bit is changed.

Note that this definition is very similar to (but a little looser than) the strict avalanche criterion [5] which states that each ciphertext bit must change with a probability of exactly one half given a particular one bit plaintext change. As a measure of a cipher's adherence to the avalanche criterion we define avalanche probability.

Definition 2 : The *avalanche probability*, P_{av}, of a cipher is the average fraction of ciphertext bits that change when one plaintext bit is changed and the key remains fixed.

For a cipher which perfectly satisfies the avalanche criterion, $P_{av} = 1/2$. The avalanche probability can be used as one measure of the performance of a cipher: the fewer rounds it takes for the avalanche probability to converge to 1/2, the stronger the cipher (with respect to avalanche), implying a cipher of more efficient construction consisting of fewer rounds.

In [4], the avalanche characteristics of basic substitution-permutation networks (SPNs) (which are not DES-like) are modelled and the effect of varying cipher parameters are examined. In this paper, we extend this work and develop a model of the avalanche characteristics of DES-like ciphers. The value of this model is that it allows us to examine the relationship between avalanche and various parameters of a DES-like cipher such as the amount of expansion and the S-box dimensions and properties. As well, the performance of DES-like ciphers and the basic SPN ciphers of [4] are compared.

II. Modelling the Cipher

As shown in Figure 1, an R-round DES-like cipher encrypts by dividing the N-bit plaintext input block into two halves: left half $\mathbf{L}_1$ and right half $\mathbf{R}_1$. [1] The right half block $\mathbf{R}_1$ is transformed by the keyed round function f and XORed bit-by-bit to the left half block $\mathbf{L}_1$ to form a new left half block. The right and left halves are then swapped. Consequently, for a round i, $1 \leq i \leq R$ of the cipher, letting $\mathbf{L}_i$ and $\mathbf{R}_i$ represent the left and right half-blocks, respectively, and $\mathbf{K}_i$ represent the key bits applied to the round function, the DES-like algorithm may be viewed as the following iterated operation:

$$\begin{aligned} \mathbf{L}_{i+1} &= \mathbf{R}_i \\ \mathbf{R}_{i+1} &= \mathbf{L}_i \oplus f(\mathbf{R}_i, \mathbf{K}_i). \end{aligned} \tag{1}$$

After the last round, since the half-blocks are not swapped, we have $\mathbf{R}_{R+1}$ and $\mathbf{L}_{R+1}$ represent-

[1] Note that the initial and final permutations of DES have been ignored.

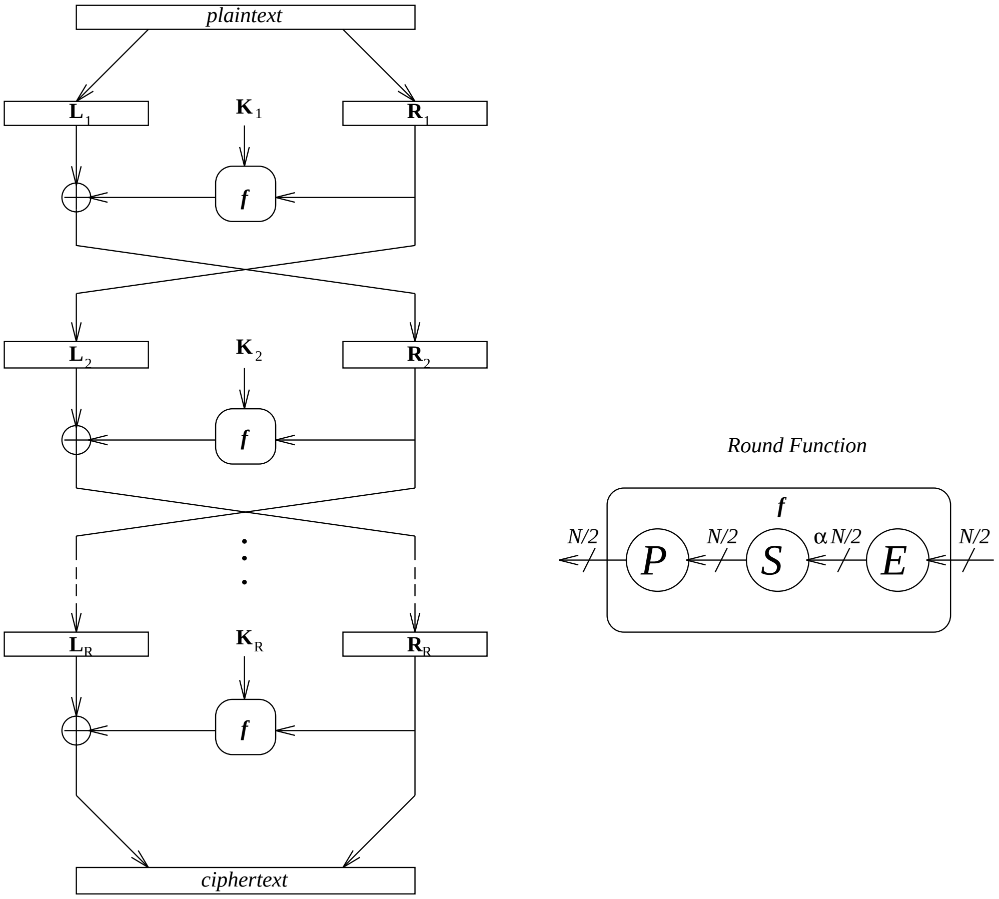

Figure 1: DES-like Cipher Structure

ing the left and right halves of the ciphertext, respectively.

As illustrated in Figure 1, there are generally three components in the round function f: the expansion (E), the substitution (S), and the permutation (P). The cipher is keyed by applying a subset of cipher key bits to the round function, typically by XORing with the data bits before the substitution is performed.

(a) S-box Model

The substitution component operates by dividing the block into a number of smaller sub-blocks and then replacing the bits of these sub-blocks according to a predefined mapping referred to as an S-box. In this paper we consider S-boxes of dimension $m \times n$, $m \geq n$, where m represents the number of input bits and n represents the number of output bits. DES has eight 6×4 S-boxes which are used in the substitution component of the round function.

In general, we represent the input to an S-box as $\mathbf{X} = [X_1 X_2 ... X_m]$, $X_i \in \{0, 1\}$, and the output as $\mathbf{Y} = [Y_1Y_2...Y_n]$, $Y_i \in \{0,1\}$. The input and output differences or change vectors of an S-box corresponding to the bit-wise XOR of two different values for $\mathbf{X}$ and the bit-wise XOR of the resulting two values for $\mathbf{Y}$ are represented by $\Delta\mathbf{X}$ and $\Delta\mathbf{Y}$, respectively.

We model the S-box in the cipher by treating the number of output changes of the S-box as a random variable. Representing the Hamming weight operation by $wt(\cdot)$ and letting $D = wt(\Delta\mathbf{Y})$ represent the random variable corresponding to the number of output bit changes, the model uses the probability distribution of D given by

$$P_D(D=0) = \begin{cases} 1 & , wt(\Delta\mathbf{X}) = 0 \\ \frac{2^{m-n}-1}{2^m-1} & , wt(\Delta\mathbf{X}) \geq 1 \end{cases} \tag{2}$$

and

$$P_D(D=d) = \begin{cases} 0 & , wt(\Delta\mathbf{X}) = 0 \\ \frac{\binom{n}{d}\cdot 2^{m-n}}{2^m-1} & , wt(\Delta\mathbf{X}) \geq 1 \end{cases} \tag{3}$$

for $1 \leq d \leq n$.

To understand the origin of (2), consider that there are 2^{m-n} times more input change vector values for $\Delta\mathbf{X}$ than output change vector values for $\Delta\mathbf{Y}$. Hence, we expect a particular value of the output change vector to occur 2^{m-n} times more often than an input change vector value. Clearly, if there are no input bit changes, then there are no output bit changes resulting the probability of 1 in the first case of (2). The remaining $2^{m-n} - 1$ occurrences of the all-zeros output change vector can be expected to occur when there are input bit changes. Since there are $2^m - 1$ non-zero input changes, the probability of a zero output change given an input change is given by the second case of (2).

Consider now the derivation of the probability distribution of D for $D > 0$ as given in (3). The first case arises from the fact that if there are no input changes, then there are no output changes and $P_D(d)$ must be zero. If there is an input change, as in the second case, then the total number of possible output changes corresponding to a weight of d is given by the number of selections of the d changes from the n output bits multiplied by the factor 2^{m-n} to account for the ratio of possible inputs to outputs. This is divided by the total number of non-zero input changes given by $2^m - 1$.

Note that this stochastic model of the S-box is not intended to characterize the behaviour of an actual, physically realizable S-box, but rather represents an aggregate behaviour over all randomly selected S-boxes. In this sense, it represents a typical S-box.

(b) Permutation Model

The permutation component transposes the bits within the block. In DES, the 32-bit permutation has the property that no two outputs of an S-box are connected to the input of the same S-box.

To model the permutation component of the round function we represent the permutation by a random variable where all possible permutations are considered equally likely. Hence, this model does not make any assumptions about the permutation properties. Instead, we model the cipher by averaging over all possible values that the permutation component can take on. Therefore, it is quite reasonable to expect that a well chosen permutation might display better characteristics than the averaging model used for the analysis. However, in general, the analysis of specific permutations is very difficult and, since the permutation depends greatly on the block and S-box sizes, it is not clear how to generalize an optimal permutation for the purposes of our model of DES-like ciphers.

(c) Expansion Model

The expansion component duplicates an appropriate number of input bits before they are presented to the substitution component and is required if asymetric $m \times n$ S-boxes with $m > n$ are used. The expansion factor, α, of the round function is given by the ratio of the number of bits entering the substitution component to the block size at the input of the round function. In DES, the round function input is 32 bits and the substitution takes 48 bits as its input. Hence DES has an expansion factor of $\alpha = 1.5$.

In our model of the avalanche characteristics of DES-like ciphers, we treat the expansion as a random variable and average over all possible values of the random variable. It is assumed that α is fixed and the expansion randomly selects the appropriate bits for duplication from the set of all bits entering the round function. For example, for the parameter values of DES, 16 out of 32 bits are arbitrarily selected as the set of duplicated bits. The model updates the avalanche characteristics based on averaging over all possible selections for those 16 bits at each round of the cipher.

III. Computation of Avalanche

In this section, we detail the computational model that is used to examine the avalanche characteristics of a cipher of R rounds. Since the avalanche probability is calculated iteratively from 1 to R rounds, ciphers may be analyzed in relation to their satisfaction of the avalanche criterion as a function of the number of rounds. Note that in the following development the key is assumed fixed and, hence, is not a factor in the computation of avalanche probability.

Consider the determination of the distribution of the number of bit changes at the input to a round given the distribution of the number of bit changes at the input to the previous round. Let η_L and η_R represent the number of bit changes in the left and right half blocks, respectively, at the input to a round i, i.e., $\eta_L = wt(\Delta\mathbf{L}_i)$ and $\eta_R = wt(\Delta\mathbf{R}_i)$. Using the total probability theorem, the probability of η_L^* and η_R^* bit changes in the left and right half inputs to round $i+1$ is given by

$$P(\eta_L^*, \eta_R^*) = \sum_{\eta_L=0}^{N/2} \sum_{\eta_R=0}^{N/2} P(\eta_L^*, \eta_R^* | \eta_L, \eta_R) \cdot P(\eta_L, \eta_R). \tag{4}$$

Since, in a DES-like structure, $\eta_L^* = \eta_R$, this can be simplified to

$$P(\eta_L^*, \eta_R^*) = \sum_{\eta_L=0}^{N/2} P(\eta_R^* | \eta_L, \eta_R = \eta_L^*) \cdot P(\eta_L, \eta_R = \eta_L^*). \tag{5}$$

Let η_f represent the number of bit changes at the output of the round function. Then

$$P(\eta_R^* | \eta_L, \eta_R) = \sum_{\eta_f=0}^{N/2} P(\eta_R^* | \eta_L, \eta_R, \eta_f) \cdot P(\eta_f | \eta_L, \eta_R). \tag{6}$$

Since η_R^* is determined directly by η_L and η_f, and η_f is not affected by η_L, we have

$$P(\eta_R^* | \eta_L, \eta_R) = \sum_{\eta_f=0}^{N/2} P(\eta_R^* | \eta_L, \eta_f) \cdot P(\eta_f | \eta_R). \tag{7}$$

Let $\mu = max(\eta_L, \eta_f)$ and $\lambda = min(\eta_L, \eta_f)$. Now $P(\eta_R^* | \eta_L, \eta_f)$ can be determined from

$$P(\eta_R^* | \eta_L, \eta_f) = \begin{cases} \dfrac{\binom{\mu}{i} \cdot \binom{N/2-\mu}{\lambda-i}}{\binom{N/2}{\lambda}} & , \eta_R^* = \eta_L + \eta_f - 2i \\ 0 & , otherwise \end{cases} \tag{8}$$

for all i, $0 \leq i \leq \lambda$. To understand the origin of (8), consider the general bit-wise XOR of two random b-bit vectors: $w = u \oplus v$ where $\eta_w = wt(w)$, $\eta_u = wt(u)$, and $\eta_v = wt(v)$. Without loss of generality, assume that $\eta_u > \eta_v$ and that the first η_u bits of u are ones and the remaining bits are zeroes. Consider now the placement of the ones in the vector v and the effect on the vector w. If i ones of the η_v ones of v are located in the first η_u bits of v, the vector w will have $\eta_u - i$ ones in the first η_u bits and $\eta_v - i$ ones in the remaining bits. Hence, $\eta_w = \eta_u + \eta_v - 2i$. The probability of $\eta_w = \eta_u + \eta_v - 2i$ given η_u and η_v is determined as the fraction of arrangements of η_v ones for which i ones are in the first η_u bits and the remaining $\eta_v - i$ ones are in the remaining $b - \eta_u$ bits. Equation (8) is derived by letting $b = N/2$, $\eta_u = \mu$, $\eta_v = \lambda$, and $\eta_w = \eta_R^*$.

Consider now the probability of the number of output bit changes given the number of input bit changes to the round function, $P(\eta_f|\eta_R)$. Let η_e represent the number of bit changes at the output of the expansion and let l represent the number of S-boxes which have at least one bit change at the input. Using total probability and the chain rule, it can be shown that

$$P(\eta_f|\eta_R) = \sum_{\eta_e=0}^{T} \sum_{l=0}^{M} P(\eta_f|l) \cdot P(l|\eta_e) \cdot P(\eta_e|\eta_R) \tag{9}$$

where T represents the number of bits at the output of the expansion component and M is the number of S-boxes in the substitution component. Hence, $T = \alpha \cdot (N/2) = M \cdot m$ represents the number of bits entering the substitution component.

The probability distribution of the number of changes at the output of the expansion given the number of input changes is given by

$$P(\eta_e|\eta_R) = \frac{\binom{T-N/2}{\eta_e-\eta_R} \cdot \binom{N-T}{2\eta_R-\eta_e}}{\binom{N/2}{\eta_R}} \tag{10}$$

where we have assumed that $T \leq N$. The first term in the numerator represents the number of selections of extra bit changes in the expanded vector from the bits that have been duplicated by the expansion function. To compute the number of arrangements of η_e bits from η_R bit changes at the expansion input, this is multiplied by the number of selections of the remaining bit changes in the expanded vector from the bits in the round function input which have not been duplicated. The probability is then calculated by dividing the number of suitable arrangements by the total number of selections of η_R bits from the round function input of $N/2$ bits.

The probability $P(l|\eta_e)$ is the probability that l S-boxes are affected by changes given that there are η_e changes at the output of the expansion component. This can be determined by computing the fraction of the number of selections of η_e bit changes that affect only l S-boxes. Letting $\mathcal{N}(\eta_e)$ represent the total number of selections of η_e bit changes and $\mathcal{N}(l,\eta_e)$ represent the number of selections that have bit changes at the input to l S-boxes, we get

$$P(l|\eta_e) = \mathcal{N}(l,\eta_e)/\mathcal{N}(\eta_e) \tag{11}$$

where

$$\mathcal{N}(\eta_e) = \left(\begin{array}{c} T \\ \eta_e \end{array} \right). \tag{12}$$

From Lemma 2 in [4], $\mathcal{N}(l,\eta_e)$ may be determined by

$$\mathcal{N}(l,\eta_e) = \sum_{i=M-l}^{M} (-1)^{i-(M-l)} \left(\begin{array}{c} i \\ M-l \end{array} \right) \left(\begin{array}{c} M \\ i \end{array} \right) \left(\begin{array}{c} (M-i)m \\ \eta_e \end{array} \right). \tag{13}$$

The probability distribution of round function output changes given the number of affected S-boxes, represented by $P(\eta_f|l)$, can be determined by counting over all combinations of output changes η_f from l S-boxes. Let $\mathbf{d} = [d_1 d_2 ... d_l]$ where $d_i \in \{1, ..., n\}$ is the number of output changes, $wt(\Delta\mathbf{Y})$, in the i-th S-box that has a non-zero input change. Now define

$$\Lambda = \{\mathbf{d} | \sum_{i=1}^{l} d_i = \eta_f\} \tag{14}$$

to represent the values of $\mathbf{d}$ for which there are a total of η_f output bit changes. Hence,

$$P(\eta_f|l) = \sum_{\mathbf{d}\in\Lambda} P(\mathbf{d}) \tag{15}$$

where $P(\mathbf{d})$ represents the probability of a particular $\mathbf{d}$ occurring and is given by

$$P(\mathbf{d}) = \prod_{i=1}^{l} P_D(d_i). \tag{16}$$

Using equations (4) to (16), we can now iteratively determine the probability distribution of bit changes, $P(\eta_L, \eta_R)$, for each round in the cipher and, subsequently, the expected number of bit changes after each round. Consequently, letting $E\{\cdot\}$ represent the expectation operation, the avalanche probability after a particular round can be determined from

$$P_{av} = E\{\eta_L + \eta_R\}/N \tag{17}$$

given $\eta_L = 1$ and $\eta_R = 0$ at the input to round 1 if the one bit change occurs in the left half of the plaintext, or $\eta_L = 0$ and $\eta_R = 1$ at the input to round 1 if the one bit change occurs in the right half of the plaintext.

IV. Analysis of the Results

In this section, we present the results of the computations of the preceding section for various ciphers with different parameters. We shall use a 64-bit cipher as a basis for comparison.

When computing the avalanche probability, one might consider one bit changes on either the left or right side of the plaintext. In fact, it can be shown that

$$P_{av}[right] = P_{av}^{*}[left] \tag{18}$$

where P_{av} and P_{av}^{*} represent the avalanche probabilities after i and $i+1$ rounds, respectively, and the keywords *left* and *right* indicate which half of the plaintext has the one bit change. This results from the fact that a one bit change on the left side manifests itself as a one bit change to the right side of the input to round 2. Since a DES-like cipher will have weaker avalanche for a bit change on the left, we shall consider the left side avalanche probability to be the property of interest.

In Figure 2, we present a plot of the avalanche probability versus the number of rounds in the cipher where the S-box dimensions are of the form $m \times 4$. Three cases are illustrated: $m = 4$, $m = 6$, and $m = 8$. All results presented are based on the plaintext bit change occurring in the left half. In all three cases, the avalanche probability is converging towards the desired value of 1/2. However, it is clear that the larger the value of m, the faster the convergence. Similar results were observed for ciphers based on $m \times 8$ S-boxes where $m = 8$, $m = 12$, and $m = 16$.

It is not surprising that performance is improved as m increases since a larger S-box input increases the diffusion of bit changes. Note also that Figure 3, which compares ciphers using 8×4 and 8×8 S-boxes, suggests that the S-boxes with larger number of outputs improve the avalanche probability convergence. Again this is perhaps not surprising and is due to the improved diffusion of bit changes. However, Figures 2 and 3 suggest that the effects of increasing the S-box input size appear to be more dramatic than an increase in the number of output bits. Unfortunately, for cipher implementations where look-up tables are used for

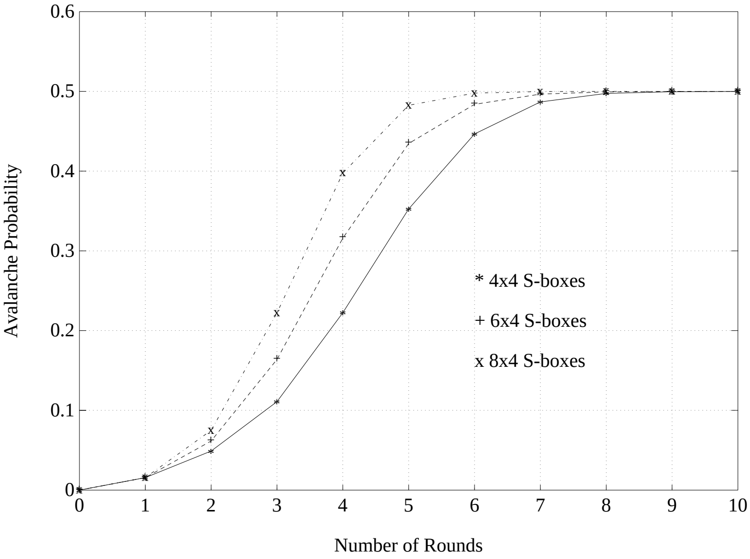

Figure 2: Theoretical Avalanche for DES-like Ciphers with $m \times 4$ S-boxes

S-boxes, the amount of memory required increases exponentially in the size of S-box input and only linearly in the size of the output. Hence, while the size of the S-box input is limited by practical considerations, the output can be more freely expanded to improve the cipher security properties. This suggests that the best combination of efficiency and security (in relation to avalanche) is given by ciphers using symmetric $n \times n$ S-boxes.

Consider now a comparison between the performance of a DES-like cipher versus a basic substitution-permutation network such as discussed in [4]. (Basic SPNs do not have the structure of Figure 1: each round consists of substitution on the entire block using N/n $n \times n$ S-boxes followed by a permutation on the entire block.) The cases for 4×4 and 8×8 S-boxes are illustrated in Figure 4. For 4×4 S-boxes there is little difference between the two ciphers. In fact, considering the relationship of (18), if the change is on the right side, then the DES-like cipher actually performs significantly better. This is perhaps surprising: since, in a basic SPN, the round function operates on the full block and, in a DES-like cipher, the round function only operates on half the block, it seems reasonable to assume that an SPN would display good cryptographic properties in fewer rounds. For the case of the larger 8×8 S-boxes, the SPN clearly has better performance than the DES-like cipher.

Of course, any cipher is a deterministic structure based on a fixed set of S-boxes, permutation

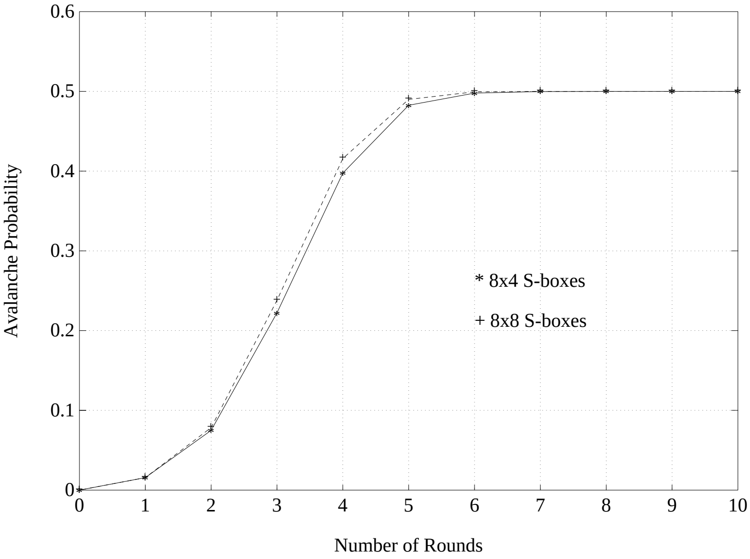

Figure 3: Theoretical Avalanche for DES-like Ciphers with 8 × 4 and 8 × 8 S-boxes

and expansion. The effect of the model, which treats these components as random variables, is to smooth out the advantages or disadvantages of particular fixed components. Although it is impossible to exactly model all ciphers using a general model, it appears that the generalizations made in this model are not only intuitively reasonable but experimental results suggest that they provide a reasonable approximation of the behaviour of a DES-like cipher. Nevertheless, it seems reasonable to expect that the model is, in fact, pessimistic and that the careful selection of S-boxes, permutations, and expansion mappings is likely to improve the performance of the cipher in relation to the avalanche characteristics [4]. In the next section, we examine the modelling of "diffusive" S-boxes and demonstrate that, indeed, S-box properties can be utilized to improve the avalanche characteristics of a DES-like cipher.

V. Improving Avalanche by Using Diffusive S-boxes

A discussion on improving the avalanche characteristics of an SPN by selecting diffusive S-boxes is contained in [4]. In this section, we consider the application of such S-boxes to a DES-like cipher. Consider the following S-box diffusion property referred to as guaranteed avalanche [4] and note that guaranteed avalanche order 2 is an acknowledged DES S-box criterion [6].

Definition 3: An S-box satifies the property of *guaranteed avalanche* of order γ if, for a one bit

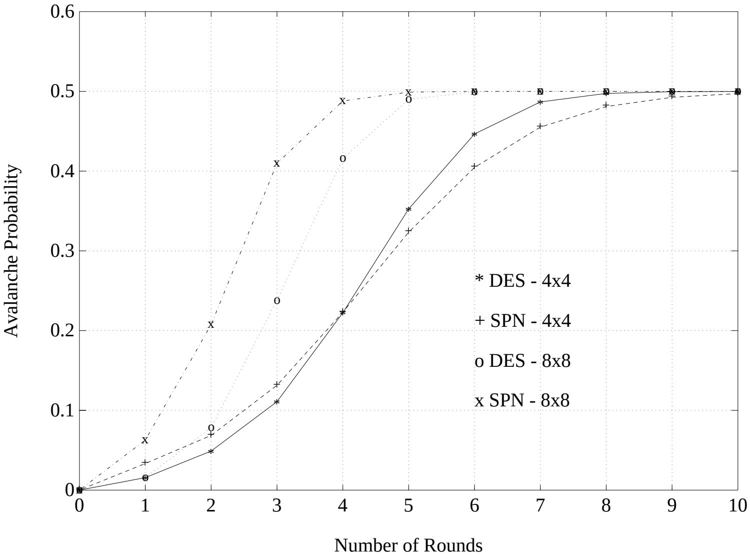

Figure 4: Theoretical Avalanche of DES-like Ciphers vs. Basic SPN Ciphers

input change, at least γ output bits change, i.e., $wt(\Delta\mathbf{X}) = 1 \Rightarrow wt(\Delta\mathbf{Y}) \geq \gamma$.

Consider now the development of a model for an S-box satisfying guaranteed avalanche order γ, $\gamma \geq 1$. The probability distribution $P_D(d)$ can be replaced by probability distributions for the number of output bit changes conditioned on the number of input changes. Clearly, $P_D(D = 0|wt(\Delta\mathbf{X}) = 0) = 1$ and $P_D(D = d|wt(\Delta\mathbf{X}) = 0) = 0$ for $d > 0$. Now let $P'_D(d) \equiv P_D(D = d|wt(\Delta\mathbf{X}) = 1)$ and $P''_D(d) \equiv P_D(D = d|wt(\Delta\mathbf{X}) > 1)$. The conditional probabilities for the number of output changes is then given by

$$P'_D(d) = \begin{cases} 0 & , d < \gamma \\ \frac{\binom{n}{d}}{\sum_{i=\gamma}^{n}\binom{n}{i}} & , d \geq \gamma \end{cases} \tag{19}$$

and

$$P''_D(d) = \begin{cases} \frac{2^{m-n}-1}{2^m-1-m} & , d = 0 \\ \frac{\binom{n}{d}2^{m-n}-mP'_D(d)}{2^m-1-m} & , d \geq 1. \end{cases} \tag{20}$$

Consider first the expression for P'_D in (19). The case of $d < \gamma$ arises simply from the definition of guaranteed avalanche; the case for $d \geq \gamma$ is derived by assuming that the selection of $\Delta\mathbf{Y}$ is uniformly distributed over the set of values such that $D = wt(\Delta\mathbf{Y}) \geq \gamma$. Considering now the expression for P''_D, the denominator of (20) represents the number of values of $\Delta\mathbf{X}$ for which $wt(\Delta\mathbf{X}) > 1$ and the numerator represents the number of values of $\Delta\mathbf{Y}$ for which $wt(\Delta\mathbf{Y}) = d$, scaled by factor 2^{m-n} and adjusted to remove the expected number of $\Delta\mathbf{Y}$ values used for the

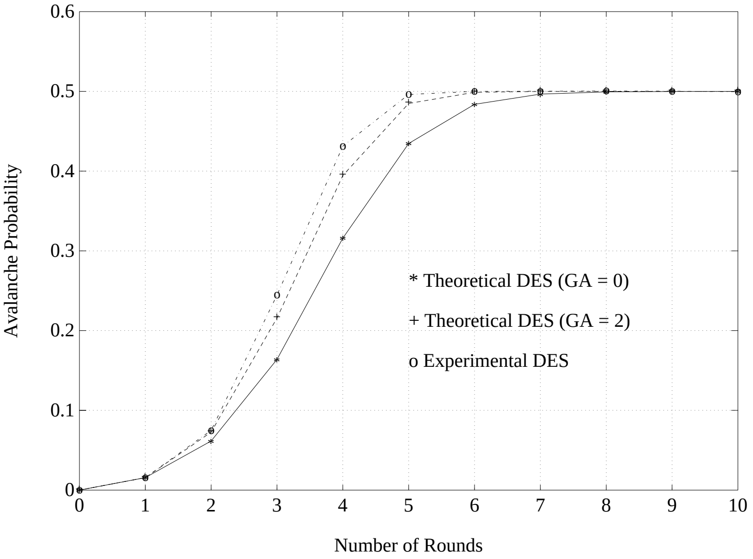

Figure 5: Avalanche for DES-like Ciphers with Diffusive S-boxes

values of $\Delta\mathbf{X}$ for which $wt(\Delta\mathbf{X}) \leq 1$.

The iterative computation of the avalanche probability follows similarly to the previous development: equations (4) through (8) are equally applicable. However, (9) must be modified to consider separately the cases of one bit input changes and more than one bit input changes to the S-boxes. Let l' represent the number of S-boxes for which $wt(\Delta\mathbf{X}) = 1$ and, as before, let l represent the number of S-boxes for which $wt(\Delta\mathbf{X}) \geq 1$. Hence, (9) becomes

$$P(\eta_f|\eta_R) = \sum_{\eta_e=0}^{T} \sum_{l=0}^{M} \sum_{l'=0}^{l} P(\eta_f|l',l) \cdot P(l',l|\eta_e) \cdot P(\eta_e|\eta_R). \tag{21}$$

The probability $P(\eta_e|\eta_R)$ may be computed as previously outlined in equation (10).

The probability $P(l',l|\eta_e)$ can be determined by

$$P(l',l|\eta_e) = \mathcal{N}(l',l,\eta_e)/\mathcal{N}(\eta_e) \tag{22}$$

where $\mathcal{N}(\eta_e)$ is the number of selections of η_e bit changes and $\mathcal{N}(l',l,\eta_e)$ is the number of selections of changes of η_e bits such that l S-boxes are affected by changes and l' S-boxes have a exactly a one bit input change. $\mathcal{N}(\eta_e)$ is given by (12) and, based on Lemma 4 in [4], $\mathcal{N}(l',l,\eta_e)$ is computed by

$$\mathcal{N}(l',l,\eta_e) = \begin{pmatrix} M \\ l \end{pmatrix} \sum_{i=l'}^{l} (-1)^{i-l'} \begin{pmatrix} i \\ l' \end{pmatrix} \begin{pmatrix} l \\ i \end{pmatrix} m^i \sum_{j=0}^{l-i} (-1)^j \begin{pmatrix} l-i \\ j \end{pmatrix} \begin{pmatrix} (l-i-j)m \\ \eta_e - i \end{pmatrix}. \tag{23}$$

In order to determine $P(\eta_f|l', l)$, define the vector $\mathbf{d}' = [d_1' d_2' ... d_{l'}]$ such that $d_i' \in \{\gamma, ..., n\}$ represents the number of output changes, $wt(\Delta\mathbf{Y})$, of the i-th S-box for which $wt(\Delta\mathbf{X}) = 1$. Similarly, define the vector $\mathbf{d}'' = [d_1'' d_2'' ... d_{l-l'}'']$ such that $d_i'' \in \{1, ..., n\}$ represents the number of output changes, $wt(\Delta\mathbf{Y})$, of the i-th S-box for which $wt(\Delta\mathbf{X}) > 1$. Then

$$P(\eta_f|l', l) = \sum_{(\mathbf{d}', \mathbf{d}'') \in \Lambda^*} P(\mathbf{d}', \mathbf{d}'') \tag{24}$$

where

$$\Lambda^* = \left\{ (\mathbf{d}', \mathbf{d}'') | \sum_{i=1}^{l'} d_i' + \sum_{i=1}^{l-l'} d_i'' = \eta_f \right\} \tag{25}$$

with the probability $P(\mathbf{d}', \mathbf{d}'')$ given by

$$P(\mathbf{d}', \mathbf{d}'') = \left[\prod_{i=1}^{l'} P_D'(d_i') \right] \left[\prod_{i=1}^{l-l'} P_D''(d_i'') \right]. \tag{26}$$

Methods for improving the efficiency of the computation are given in [4].

Similarly to the previous development, (4) can be used to iteratively compute the avalanche probability given a plaintext bit change in either the left or right half. For example, results have been computed for a 64-bit cipher using 6 × 4 S-boxes, both for the original S-box model with no diffusion (i.e., $\gamma = 0$) and for the S-box model based on guaranteed avalanche order $\gamma = 2$. This is illustrated in Figure 5. There is a clear improvement in the avalanche performance for the cipher constructed using diffusive S-boxes over a cipher without difffusive S-boxes. As well, for comparison, since DES S-boxes satisfy $\gamma = 2$, experimental results for DES based on 10^4 pairs of plaintexts are also shown. While the theoretical and experimental results for DES are close, it is not surprising that experimental results on DES are slightly better than the theoretical model with diffusive S-boxes. To more accurately model DES, the model would have to incorporate a fixed representation of the DES expansion and permutation instead of treating the expansion and permutation as random and averaging over all possibilities, good and bad.

VI. Conclusion

We have modelled the avalanche characteristics for DES-like block ciphers and, consequently, analyzed the performance of the ciphers in response to variations in parameters such as the

S-box dimensions and properties. The results suggest that large, symmetric S-boxes provide the best combination of cipher efficiency and the strength of a cipher's avalanche. As well, the model is extended and used to demonstrate that selecting diffusive S-boxes is also effective in improving the avalanche characteristics of a DES-like cipher.

References

[1] H. Feistel and W.A. Notz and J.L. Smith, "Some cryptographic techniques for machine-to-machine data communications", *Proceedings of the IEEE*, vol. 63, no. 11, pp. 1545-1554, 1975.

[2] "Data Encryption Standard (DES)", *Federal Information Processing Standard Publication 46*, National Bureau of Standards, 1977.

[3] H. Feistel, "Cryptography and computer privacy", *Scientific American*, vol. 228, no. 5, pp. 15-23, 1973.

[4] H.M. Heys and S.E. Tavares, "Avalanche characteristics of substitution-permutation encryption networks", *IEEE Transactions on Computers*, vol. 44, no. 9, pp. 1131-1139, 1995.

[5] A.F. Webster and S.E. Tavares, "On the design of s-boxes", *Proceedings of CRYPTO '85*, Springer-Verlag, Berlin, pp. 523-534, 1986.

[6] E.F. Brickell and J.H. Moore and M.R. Purtill, "Structures in the s-boxes of DES ", *Advances in Cryptology: Proceedings of CRYPTO '86*, Springer-Verlag, Berlin, pp. 3-8, 1987.