An Expanded Set of S-box Design Criteria Based on Information Theory and its Relation to Differential-Like Attacks

M. H. Dawson and S. E. Tavares

Department of Electrical Engineering
Queens University at Kingston
Kingston, Ontario, Canada, K7L 3N6
Phone (613) 545–2925
Fax (613) 545–6615

Abstract

The security of DES-like cryptosystems depends heavily on the strength of the Substitution boxes (S-boxes) used. The design of new S-boxes is therefore an important concern in the creation of new and more secure cryptosystems. The full set of design criteria for the S-boxes of DES has never been released and a complete set has yet to be proposed in the open literature. This paper introduces a unified S-box design framework based on information theory and illustrates how it provides immunity to the differential attack.

Introduction

In private-key cryptosystems which are based on substitution-permutation (S-P) networks (i.e., DES-like systems), the strength of the cryptosystem depends directly on the quality of the substitution boxes (S-boxes) used by the algorithm. Biham and Shamir, in their recent paper on Differential Cryptanalysis [1] showed that DES could be broken if poor S-boxes were used. The design of good S-boxes is therefore an important part of designing a DES-like cryptosystem.

In this work we present an expanded set of design criteria for creating good S-boxes based on information theoretic concepts and show that an S-Box that meets these criteria is immune to differential cryptanalysis[1]. We also discuss the analysis of the DES S-boxes and the creation of new S-boxes of various sizes using the new design framework. The new criteria give us new insights into the design of good S-boxes which is of considerable interest as any new private-key cryptosystem that replaces DES will require new S-boxes for copyright and security reasons.

Background

Cryptographic substitutions, first introduced by Shannon in [2], were further refined and explained in [3][4]. It has been shown in [5][6] and more recently in [1] that poor S-boxes can lead to weak cryptosystems. The S-boxes of DES [7] have been subject to much analysis (see [8][9][10][11] and others).

Work on defining desirable properties of S-boxes has been presented in [12][13][14] [15][16][17]. More recently, some properties based on information theory were presented by Forré in [11]. Despite the previous investigations of desirable properties of S-boxes, a comprehensive set of design criteria for S-boxes has yet to be presented.

D.W. Davies (Ed.): Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp. 352-367, 1991.

We will extend the set of desirable properties of S-boxes using information theory and use these properties to propose a set of design criteria for S-boxes.

Static and Dynamic Views of an S-box

S-Boxes can be viewed in two distinct ways. The first is the static view of the S-box which describes the S-box when the inputs are not changing. The second is the dynamic view of the S-box which describes the S-box when the inputs are changing.

Much of the previous work on S-boxes has focussed on the static properties of S-boxes. The static view of an S-box, with inputs $\mathbf{X} = [x_1, ..., x_m]$ and outputs $\mathbf{Y} = [y_1, ..., y_n]$, can be envisioned as shown in Figure 1.

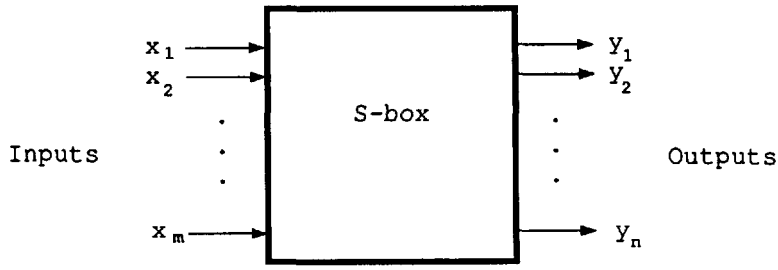

Figure 1 Static View of an m×n S-box

The importance of certain **dynamic** properties of an S-box were introduced by Feistel in [3] and refined in [14]. More recently Biham and Shamir's work on differential cryptanalysis[1] stimulated us to discover that a broader range of dynamic properties of S-boxes are important in DES-like cryptosystems. When considering the dynamic properties of an S-box, it is useful to refer to the delta S-box shown in Figure 2.

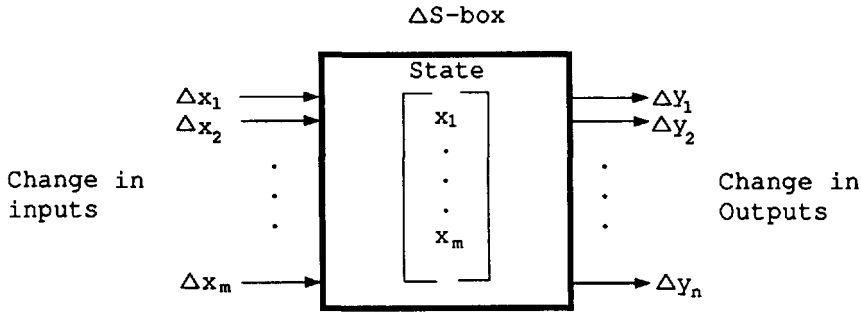

Figure 2 Dynamic View of an m×n S-box

In Figure 2 the values of the vector $\mathbf{X} = [x_1, ..., x_m]$ are the current inputs to the S-box and can be viewed as the state of the delta S-Box. The Δx_i and the Δy_i are the changes in the inputs and outputs respectively. The current state **X** is usually unknown and it is assumed that any relation found between the Δx_i and the Δy_i is over all possible states.

Properties of Ideal S-boxes Based on Information Theory

For a random variable z with possible values $z_1, ..., z_n$, the uncertainty in z is $H(\mathbf{z}) = \sum_{i=1}^{n} P(z_i) log_2\left(\frac{1}{P(z_i)}\right)$. The mutual information between two random variables X and Y is $I(\mathbf{X};\mathbf{Y}) = H(\mathbf{X}) - H(\mathbf{X} \mid \mathbf{Y})$. The information theoretic basis for our criteria is to minimize the information which can be gained about unknown inputs and outputs of an S-box from known inputs and outputs. If the random variable U describes the known values and the random variable V represents the unknown values we want $I(\mathbf{V};\mathbf{U}) = H(\mathbf{V}) - H(\mathbf{V} \mid \mathbf{U}) = 0$. An "Ideal" S-box should have $I(\mathbf{V};\mathbf{U}) = 0$ for U representing any combination of the inputs and outputs. However, due to the deterministic nature of an S-box the input-output relation is known. The best an Ideal S-box can do then is to have $I(\mathbf{V};\mathbf{U}) = 0$ when U represents any combination of a subset of the inputs and a subset of the outputs. By minimizing the information which leaks through the S-box the amount of information available to a cryptanalyst is reduced and thus the cryptosystem is strengthened. In [11] Forré developed two properties of an Ideal m×n bit S-box based on these ideas. The first property was that the uncertainty in the output bits is not reduced by the knowledge of any subset of the input bits. The second property was that the uncertainty in any unknown output bits is not reduced by the knowledge of the other output bits.

We have defined a set of six properties that an Ideal S-box is required to meet. This set of properties has a broader scope than those of Forré and any S-box that meets these properties will also meet Forré's. The properties are grouped into a set of static properties and a set of dynamic properties.

Static Properties

The first static property is that the partial information about the inputs and outputs does not reduce the uncertainty in an unknown output. Note that this is a stronger property than Forré's because partial knowledge about the output is also given. More formally, the first static property is that:

$$H(y_i \mid x_{j_1}, ..., x_{j_k}, y_{l_1}, ..., y_{l_s}) = H(y_i)$$

for all $i, k, l, s, p \mid 1 \leq i \leq n, 1 \leq k \leq m-1, 1 \leq j_1, ..., j_k \leq m, 1 \leq s \leq n-1, 1 \leq (l_1, ..., l_s, p) \leq n, l_p \neq i$.

The second static property is that the partial information about the inputs and outputs does not reduce the uncertainty in an unknown input. This property is required because the S-box can often be attacked from both the input and output directions. Note that this is a stronger property than Forré's because partial knowledge about the input is also given. More formally, the second static property is that:

$$H(x_i \mid x_{j_1}, ..., x_{j_k}, y_{l_1}, ..., y_{l_s}) = H(x_i)$$

for all $i, k, l, s, p \mid 1 \leq i \leq m, 1 \leq k \leq m-1, 1 \leq (j_1, ..., j_k, p) \leq m, 1 \leq s \leq n-1, 1 \leq l_1, ..., l_s \leq n, j_p \neq i$.

The third static property is that the uncertainty in a data value is reduced by the minimum amount possible when it passes through an S-box. This means that uncertainty in the output of the S-box is as great as the uncertainty in the input of the S-box, and if this is not possible, because m > n, that the uncertainty in the output is the maximum for the number of output bits. This property is desirable so that one cannot guess the output of the S-box more easily that the input. More formally, let $\mathbf{X} = [x_1, ..., x_m]$, $\mathbf{Y} = [y_1, ..., y_n]$ where $m \geq n$, then the third static properties is that:

$$H(\mathbf{Y}) = \begin{Bmatrix} H(\mathbf{X}), & if\ H(\mathbf{X}) \leq n \\ n, & if\ H(\mathbf{X}) > n \end{Bmatrix}$$

Dynamic Properties

The dynamic properties are similar to the static properties except that they deal with the changes in the inputs and outputs. These definitions refer to the delta S-box. The first dynamic property is that partial information about the changes in the inputs and outputs does not reduce the uncertainty in changes of the unknown outputs. More formally, the first dynamic property is that:

$$H(\Delta y_i \mid \Delta x_{j_1}, ..., \Delta x_{j_k}, \Delta y_{l_1}, ..., \Delta y_{l_s}) = H(\Delta y_i)$$

for all $i, k, l, s, p \mid 1 \leq i \leq n, 1 \leq j_1, ..., j_k, k \leq m, 1 \leq s \leq n-1, 1 \leq (l_1, ..., l_s, p) \leq n, l_p \neq i$.

The second dynamic property is that partial information about the changes in the inputs and outputs does not reduce the uncertainty in changes of the unknown inputs. Again, this property is required because an S-box may be attacked from both the input and output directions. More formally, the second dynamic property is that:

$$H(\Delta x_i \mid \Delta x_{j_1}, ..., \Delta x_{j_k}, \Delta y_{l_1}, ..., \Delta y_{l_s}) = H(\Delta x_i)$$

for all $i, k, l, s, p \mid 1 \leq i \leq m, 1 \leq k \leq m-1, 1 \leq (j_1, ..., j_k, p) \leq m, 1 \leq l_1, ..., l_s, s \leq n, j_p \neq i$.

The third dynamic property is that the uncertainty in the changes in a data value is reduced by the minimum amount possible when it passes through an S-box. This means that uncertainty in the output changes of the S-box is as great as the uncertainty in the input changes of the S-box, and if this is not possible, because m > n, that the uncertainty in the output changes is the maximum for the number of output bits. This property is desirable so that one cannot guess the output changes of the S-box more easily that the input changes. More formally, let $\Delta\mathbf{X} = [\Delta x_1, ..., \Delta x_m]$, $\Delta\mathbf{Y} = [\Delta y_1, ..., \Delta y_n]$ where $m \geq n$, then the third dynamic property is that:

$$H(\Delta\mathbf{Y}) = \begin{Bmatrix} H(\Delta\mathbf{X}), & if\ H(\Delta\mathbf{X}) \leq n \\ n, & if\ H(\Delta\mathbf{X}) > n \end{Bmatrix}$$

Again, this property is important to ensure that repeated use of S-boxes does not reduce the uncertainty in the changes of the outputs of the S-boxes and therefore reduce the work required for cryptanalysis.

Static Design Criteria

This section defines the static design criteria for m×n S-boxes which are based on the static properties of an Ideal S-box. Note that invertibility only applies to n×n S-boxes. The definitions are for an m×n bit S-box with inputs **X** and outputs **Y**. In the definition of the design criteria we use the requirement that $P(u_j \mid \mathbf{V}) = P(u_j)$ to enforce that $I(\mathbf{U}; \mathbf{V}) = 0$. This is the same as requiring that $H(\mathbf{U}) - H(\mathbf{U} \mid \mathbf{V}) = 0$. We chose this description because it makes the implications of the criteria clearer.

Input-output Independence

The Input-output Independence criterion of order r is used to select S-boxes for which knowledge of r input values does not reduce the uncertainty in the output values. Formally, an S-box meets the Input-output Independence criterion of order r, r < m, iff:

$$Prob(y_j \mid a_1 x_1, ..., a_m x_m) = Prob(y_j)$$

for all $x_i, y_j, a_k \mid 1 \leq j \leq n, 1 \leq i,k \leq m, (a_k, x_i, y_j) \in \{0,1\}, A = [a_1, ..., a_m], W(A) = r$, where $a_k = 1$ denotes that x_k is given and $a_k = 0$ denotes that x_k is not given. Note that the highest order of Input-output Independence that can be met is m-1. To meet Input-output Independence of order m the input-output relation would have to be unknown and this is never true due to the deterministic nature of S-boxes.

Output-input Independence

The Output-input Independence criterion is used to select S-boxes for which knowledge of some of the outputs does not reduce the uncertainty in the inputs. This criterion is defined in exactly the same way as Input-output Independence except that the inputs and outputs are reversed.

Output-output Independence

The Output-output Independence criterion is used to select S-boxes for which partial information about the outputs bits does not reduce the uncertainty in the unknown output bits. Formally, an S-box meets the Output-output Independence criterion of order r, r < n, iff:

$$Prob(y_j \mid a_1 y_1, ..., a_n y_n) = Prob(y_j)$$

for all $y_j, a_k \mid 1 \leq j,k \leq n, (a_k, y_j) \in \{0,1\}, a_j = 0, A = [a_1, ..., a_n], W(A) = r$, where $a_k = 1$ denotes that x_k is given and $a_k = 0$ denotes that x_k is not given. This criterion is important in order to prevent attacks which use correlation between the outputs of the S-boxes from succeeding.

An important result which we discovered is that this criterion is met, for all orders of n-1 or less, by all invertible n×n bit S-boxes. The proof is quite simple and is as follows. The possible outputs of an invertible n×n bit S-box include all the values from 0 to $2^n - 1$. For this reason if the output value $y_1, y_2, ..., y_{l-1}, 1, y_{l+1}, ..., y_n$ exists, the value $y_1, y_2, ..., y_{l-1}, 0, y_{l+1}, ..., y_n$ must also exist and therefore the values of y_i , $i \neq l$ cannot be used to predict the value of y_l. It follows that the output bits of an invertible S-box are independent. This proof can be extended to show that any m×n bit S-box made up of invertible n×n bit S-boxes meets the Output-output Independence criterion for all orders up to n-1 because, assuming all input values occur, each possible output value will occur 2^{m-n} times and thus the same argument holds except that the output values $y_1, y_2, ..., y_{l-1}, 1, y_{l+1}, ..., y_n$ and $y_1, y_2, ..., y_{l-1}, 0, y_{l+1}, ..., y_n$ each occur 2^{m-n} times.

Nonlinearity

Nonlinearity is a crucial property of an Ideal S-box. It is the nonlinearity of an S-box that prevents it from being expressed as a set of linear equations, which could then be used to break any cryptosystem using that S-box. It is therefore important to use S-boxes with the highest possible nonlinearity. Nonlinearity has been proposed as a design criterion previously and is defined in [12].

Information Completeness

The criterion of Completeness was proposed by Kam and Davida in [13]. They define Completeness as:

for every possible input value every output bit depends on all input bits and not just a proper subset of the input bits.

As noted by Forré in [11] this is a weak concept. We extend this definition, to define *Information Completeness*, by requiring that each output bit depend on all the information in each input bit as opposed to depending on only part of the information in each bit. This means that no function of the inputs, whose output set has less information content than the original set of inputs, can produce the

same set of outputs for the S-box. In Figure 3 this means that if the set $\mathbf{X}' = \{x_1', ..., x_m'\}$ produced by the mapping $F(\mathbf{X}) = \mathbf{X}'$, produces the same outputs, from the S-box, as the set $\mathbf{X} = \{x_1, ..., x_m\}$ and has less information content than X, the S-box is not Information Complete.

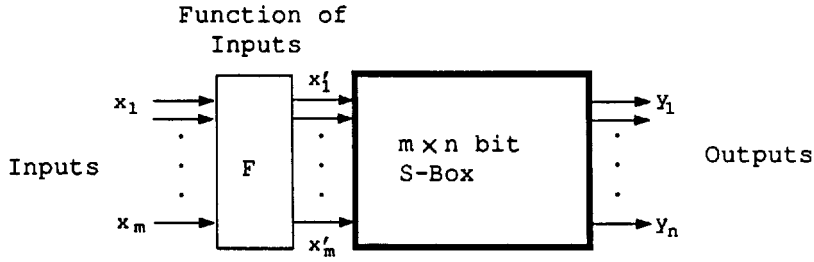

Figure 3 Illustration of Information Completeness for an m×n bit S-box

More formally, an m×n S-box, S, will be Information Complete iff there exists no function F such that: $\mathbf{F}(\mathbf{X}) = \mathbf{X}'$ and

$$H(\mathbf{X}') < H(\mathbf{X})$$

and $S(\mathbf{X}') = S(\mathbf{X})$ for all values of X.

It is clear that Information Completeness includes the notion of Completeness because if any output bit of the S-box does not depend on input bit k, the function:

$$F_{inc}(x_1, ..., x_m) = (x_1, ..., x_{k-1}, x_k, x_{k+1}, ..., x_m),\ x_k = 0$$

exists and $H(F_{inc}(\mathbf{X})) < H(\mathbf{X})$ *and* $S(F_{inc}(\mathbf{X})) = S(\mathbf{X})$ for all values of X, and therefore the S-box will fail the test of Information Completeness.

This criterion is proposed because all Ideal S-boxes are Information Complete. In the case where an output only depends on a subset of the inputs, partial information (the inputs that the output depends on) can be used to reduce the uncertainty in the output value. This is also the case if the output depends on all the inputs but only on part of the information in the inputs. As an example, consider a 4×4 bit S-box that is not Information Complete and that the Function $F(x_1, x_2, x_3, x_4) = F(x_1, x_2, x_3 + x_4, x_4)$ exists whose outputs produce the same values for output1 of the S-box as $x_1, ..., x_4$(+ is the standard inclusive or function). In this case the uncertainty in output1 of the S-box is reduced by the partial information of the values of x_1, x_2, x_4. This is because the value of $x_3 + x_4$ can be guessed with probability greater than 1/2. Any S-box that meets the third static property of an Ideal S-box must be Information Complete.

This criterion is important because if an S-box is not Information Complete the outputs may be reduced to a function of fewer inputs (it can be produced by a smaller S-box), and this will reduce the strength of the system as smaller S-boxes have poorer properties than larger ones.

Invertibility

This criterion is generally known to be a desirable property of n×n S-boxes. An S-box is invertible iff it is a one to one mapping. More formally, an n bit S-box, S, is invertible iff:

$$S(\mathbf{X_1}) = S(\mathbf{X_2})\ \ iff\ \ \mathbf{X_1} = \mathbf{X_2}$$

for all inputs $\mathbf{X_1}$ *and* $\mathbf{X_2}$. This criterion fits into our information theoretic framework because an Ideal n×n S-box must meet this criterion. If an S-box is not invertible there are fewer output values than there are input values. If there are fewer output values than input values then there is less uncertainty in the output than in the input, and therefore the third static property of an Ideal S-box will not be met.

Dynamic Design Criteria

The following section defines the dynamic design criteria for m×n S-boxes. The definitions are for an m×n bit S-box with inputs X and outputs Y and use the concept of the delta S-box with changes to the inputs Δx and changes to the outputs Δy.

Dynamic Input-output Independence

The Dynamic Input-output Independence criterion, of order r, is used to select S-boxes for which knowledge of the changes in r inputs bits, does not reduce the uncertainty in the changes of the outputs. Formally, an S-box meets the Dynamic Input-output Independence criterion of order r, $r \leq m$ iff:

$$Prob(\Delta y_j \mid a_1 \Delta x_1, ..., a_m \Delta x_m) = Prob(\Delta y_j)$$

for all $\Delta x_i, \Delta y_j, a_k \mid 1 \leq j \leq n, 1 \leq i, k \leq m, (a_k, \Delta x_i, \Delta y_j) \in \{0,1\}, A = [a_1, ..., a_m], W(A) = r$, where $a_k = 1$ denotes that Δx_k is given and $a_k = 0$ denotes that Δx_k is not given. This criterion is related to previous work in that the Strict Avalanche Criterion introduced and defined by [14, 18] and its extensions are a subset of Dynamic Input-output Independence of order m. The Strict Avalanche Criterion is met if:

$$Prob(\Delta y_j \mid \Delta x_1, ..., \Delta x_m) = Prob(\Delta y_j)$$

for all $\Delta x_i, \Delta y_j \mid 0 \leq j \leq n, 1 \leq i, k \leq m, (\Delta x_i, \Delta y_j) \in \{0,1\}, \Delta X = [\Delta x_1, ..., \Delta x_m], W(\Delta X) = 1$, and the extension to order r, $r \leq m$, is met if:

$$Prob(\Delta y_j \mid \Delta x_1, ..., \Delta x_m) = Prob(\Delta y_j)$$

for all $\Delta x_i, \Delta y_j \mid 0 \leq j \leq n, 1 \leq i, k \leq m, (\Delta x_i, \Delta y_j) \in \{0,1\}, \Delta X = [\Delta x_1, ..., \Delta x_m], W(\Delta X) = r$.

The requirements of SAC are clearly a subset of the requirements of Dynamic Input-output Independence of order m. The extension of SAC given above is also a subset of Dynamic Input-output Independence of order m as it simply enlarges the set of the values of $(\Delta x_1, ..., \Delta x_m)$ for which the condition must hold. In the extreme case, SAC of order m = Dynamic Input-output Independence of order m. We want it to be clear that Dynamic Input-output Independence is not a direct extension of SAC because it originated from a completely different viewpoint, but that SAC happens to be a subset of the highest order of it.

Dynamic Output-input Independence

The Dynamic Output-input Independence criterion is used to select S-boxes for which knowledge of some of the output changes does not reduce the uncertainty in the input changes. This criterion is defined in exactly the same way as Dynamic Input-output Independence except that the input changes and output changes are reversed.

Dynamic Output-output Independence

The Dynamic Output-output Independence criterion, of order r, is used to specify S-boxes for which the knowledge of r of the output changes and a particular pattern of input changes, does not reduce

the uncertainty in the unknown output bits. Formally, an S-box meets the Dynamic Output-output Independence criterion of order r, r < n, iff:

$$Prob(\Delta y_j \mid a_1\Delta y_1, ..., a_n\Delta y_n, \Delta x_1, ..., \Delta x_m) = Prob(\Delta y_j \mid \Delta x_1, ..., \Delta x_m)$$

for all $\Delta x_i, \Delta y_j, a_k \mid 1 \leq j \leq n, 1 \leq i,k \leq m, (a_k, \Delta x_i, \Delta y_j) \in \{0,1\}, a_j = 0, A = [a_1, ..., a_m], W(A) = r$, where $a_k = 1$ denotes that Δx_k is given and $a_k = 0$ denotes that Δx_k is not given.

Resistance to Differential Cryptanalysis.

Biham and Shamir introduced differential cryptanalysis in [1]. The attack is based on using the imbalances in the "pairs XOR distribution table", for an S-box, to predict the output XOR from the input XOR. Consider an m×n S-box that meets the Dynamic Input-output Independence criterion of order m and the Dynamic Output-output Independence criterion of order n–1. Since no information about the output changes can be gained from the knowledge of the input changes, each output XOR must occur with equal probability for each input XOR. The "pairs XOR distribution table", for an m×n S-box meeting the Dynamic Input-output Independence criterion of order m would be as shown in Figure 4.

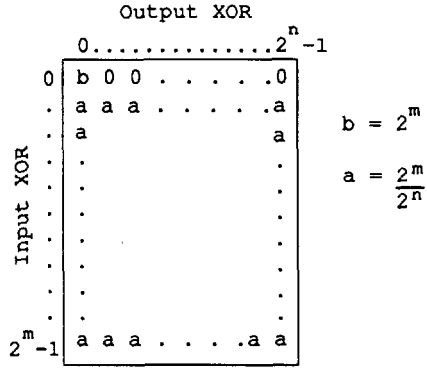

Figure 4 XOR Distribution Table for an S-box which Meets the Dynamic Input-output and Output-output Independence Criteria.

It is clear that the freedom from imbalances in the "pairs XOR distribution table" shown in Figure 4 makes the S-box immune from the differential attack. Any m×n S-box that meets the Dynamic Input-output Independence criterion of order m and the Output-output Independence criterion of order n–1 is therefore immune to the differential attack.

Avalanche Criteria

Many of the previously proposed design criteria for S-boxes are used to ensure that the cryptosystem in which they are used possess certain kinds of avalanche. We do not view the properties which these criteria require as fundamental properties of S-boxes, however they may be necessary when S-boxes are used in certain types of cryptosystems. The avalanche properties can be divided into three classes: Probabilistic Avalanche, Directed Avalanche, and Minimal Avalanche. *Probabilistic Avalanche* criteria require that each output of an S-box change with probability 1/2 whenever the input is changed. The changes in the outputs must also be independent. All S-boxes which meet the dynamic information theoretic criteria will posses Probabilistic Avalanche and this is regarded as the only type of avalanche

which is a fundamental property of a good S-box. *Directed Avalanche* criteria require that each output of an S-box change with probability 1/2 whenever certain patterns of change are made in the input. Again, the changes in the output bits must be independent. Examples of Directed Avalanche criteria are the Strict Avalanche Criterion (SAC) and all of its extensions. *Minimal Avalanche* criteria require that a minimum number of output bits changes when certain patterns of change are made in the input. The DES design criteria that requires that at least two output bits change when one input is changed is a good example of a Minimal Avalanche criterion. Neither Minimal nor Directed avalanche properties are fundamental to good S-boxes, however they may be useful whenever smaller S-boxes are used to create the larger substitutions required in SP network based cryptosystems. When smaller S-boxes are used in SP network based cryptosystems, the permutations used ensure that the outputs of individual S-boxes are distributed to the inputs of distinct S-boxes in the next round. This distribution has the effect of forcing certain patterns of changes in the input (those where 1 or 2 bits change) to be the most likely to occur in the early rounds. Due to this effect it is justified to used Minimal or Directed avalanche criteria to ensure that adequate avalanche will occur for those patterns of change. In other cryptosystems where all of the patterns of change in the inputs are equally likely it does not make sense to require Minimal or Directed Avalanche.

Application of the Criteria

The evaluation of S-boxes using the set of information theoretic design criteria would be simple if all of the criteria could be met simultaneously. In this case either the S-box would meet all the criteria and be acceptable or it would not. Unfortunately, all the criteria cannot be met simultaneously. We must therefore formulate a measure of how close an S-box comes to meeting each of the design criteria. This approach is somewhat new as most of the previous criteria were proposed on a pass/fail type of evaluation. Dropping the requirement that S-boxes meet a particular criterion perfectly complicates the evaluation and design of S-boxes. There are many possible ways to measure the criteria and the formulation of the method used to evaluate an S-box based on all the criteria simultaneously requires some difficult decisions. Since we based our criteria on information theoretic ideas, the natural basis for the required measures is information theory. For the criteria which require a form of independence, such as Input-output Independence, the measure used will be the average amount of information revealed about the unknown bits by the knowledge of partial information about the other bits. This is simply a measure of the average mutual information between the known input or output bits of the S-box and the unknown input or output bits. We will refer to this measure as the *Information Leakage measure* to emphasize that an increase in mutual information is undesirable and that for an Ideal S-box all the measures would be zero. To illustrate how this measure is used to judge how close an S-box comes to meeting the criteria, consider the Input-output Independence criterion. The Information Leakage measure for the Input-output Independence criterion of order 1 is the average amount of information revealed about an output bit by the knowledge of one input bit. Similarly, the Information Leakage measure for the Input-output Independence criterion of order 2 is the average amount of information revealed about an output bit by the knowledge of two input bits. The measures for the higher orders of the criterion are defined in the same manner. The design criteria which will be evaluated using the Information Leakage measure are :

1. Input-output Independence
2. Output-input Independence
3. Output-output Independence
4. Dynamic Input-output Independence

5. Dynamic Output-input Independence
6. Dynamic Output-output Independence

Each of the three remaining criteria will be evaluated using different methods.

Nonlinearity will be measured in the normal way as defined by Pieprzyk and Finkelstein [12]. The nonlinearity of each individual vector will be measured as its Hamming distance from the closest linear vector. In previous analyses of the nonlinearity of DES [12], it seems that the measure used to judge the nonlinearity of the 6×4 bit DES S-boxes was formed by adding the nonlinearities of the four 4×4 bit sub S-box vectors for each output of a 6×4 bit DES S-box. We feel that a better measure for the nonlinearity of the 6×4 bit S-box vectors is to compute the hamming distance of the complete output vector from the closest linear vector of the same length. This method produces the true nonlinearity of the 6×4 bit S-box vectors (which can be greater than 16) and is therefore a better measure of nonlinearity for these vectors.

The Information Completeness criterion will be evaluated using a set of measures. Each measure will be calculated to be the average information in k input bits on which the output of the vector does not depend. This measure will be referred to as the *Information Degeneracy measure* to emphasize that the measures for an Ideal S-box would all be zero. As an example, the Information Degeneracy measure of order 1 is the average amount of information in an individual input bit on which the output bit does not depend. Similarly, the Information Degeneracy measure of order 2 is the average amount of information in a pair of input bits on which the output bit does not depend and so on for the other orders. The Information Degeneracy measure is only meaningful up to order m-1 for an m×n bit S-box.

There will be no measure for the criterion of Invertibility because an S-box is either invertible or it is not.

Analysis of DES S-boxes Using The Design Criteria

We first applied the new design framework to analyze the DES S-boxes. We investigated both the properties of the DES 6×4 bit S-boxes and the DES 4×4 S-boxes. The investigations revealed that we could not find S-boxes with substantially better information theoretic properties than the S-boxes of DES and which also meet the acknowledged DES design criteria. This indicates that the S-boxes of DES may be some of the best possible based on a combination of our information theoretic properties and the acknowledged DES design criteria. It is important to note that there were many S-boxes found which met the acknowledged DES design criteria but had poor information theoretic properties.

It was also revealed that the properties of the inverses of the DES 4×4 S-boxes were as good as those of the S-boxes themselves. In addition, we discovered that the inverses of the DES 4×4 S-boxes meet the acknowledged DES design criterion which requires that at least two bits change in the output whenever one input bit is changed. These two discoveries indicate that the designers of DES placed an equal emphasis on the properties of the S-boxes and their inverses.

In every case we found that the properties of the complete 6×4 S-boxes were better than any individual 4×4 sub-box. We concluded that using multiple sub-boxes to form a larger S-box is an important method which can be used to create S-boxes that have better properties than are possible in a single sub-box. This gives a possible explanation for why multiple sub-boxes were used to create the S-boxes of DES. Some of the unexplained DES design criteria may have been included to ensure that the properties of the S-boxes created from the 4×4 S-boxes were acceptable.

One important fact noted in this investigation is that no n×n S-box can meet the Dynamic criteria perfectly because, due to the nature of the XOR function, output XOR values always occur in pairs (since $a \oplus b = b \oplus a$).

Further details of the investigations into the properties of the S-boxes of DES are contained in [19]

Creation of New DES-like S-boxes

The second application for our the new design framework was to design new S-boxes. In order to further evaluate the DES S-boxes we first chose to create S-boxes which met the acknowledged DES design criteria and met our criteria as well as the S-boxes of DES. These S-boxes will be called *DES-like*. We created over 12000 new 4×4 DES-like S-boxes and 257 new 6×4 DES-like S-boxes. During the process of creating these new S-boxes we discovered several important results. First, the inverse of an S-box with good information theoretic properties does not necessarily have good properties. Second, that there are many S-boxes which met the acknowledged DES design criteria which have poor information theoretic properties. Last, we found no S-boxes, of similar size, which had significantly better information theoretic properties than the S-boxes of DES. These results indicate that our set of criteria impose different requirements than the acknowledged DES design criteria and that it is not likely that the good information theoretic properties exhibited by the S-boxes of DES and their inverses is accidental.

Creation of other new S-boxes

Since we do not believe that the Minimal Avalanche requirements of DES are fundamental to all good S-boxes we wanted to check if S-boxes with better information theoretic properties could be created if the requirements of the acknowledged DES design criteria were removed. We created many new 4×4 and 6×4 S-boxes which did not meet the acknowledged DES design criteria but that possessed better information theoretic properties. This result suggests that care should be taken when choosing the required avalanche criteria so that one does not reduce the attainable information theoretic properties.

There is considerable interest in the creation of larger S-boxes. In order to demonstrate that our design framework could be used to create larger S-boxes we produced more than fifty 5×5 bit S-boxes using two methods which are applicable to the construction of larger S-boxes. Further details about these methods is available in [19, 20]

Comparision of Information Theoretic Properties

As a final demonstration that our new criteria impose requirements on the design of S-boxes which differ from those proposed in previous work we will present the values of the Information theoretic values for four 4×4 S-boxes. The first was generated at random, the second was listed in [14] by Webster, the third is a sub-box of the first DES S-box, and the last is a new S-box we created. The measures of the information theoretic properties of these S-boxes appear in Figures 5 to 8. From the measures given for each S-box it should be clear that using our design framework results in S-boxes with better information theoretic properties.

```
S-BOX vectors
-------------
0001010110100111  Nonlin:4    Inverse Nonlin:4
1100000010011111  Nonlin:4    Inverse Nonlin:2
1001101000110110  Nonlin:4    Inverse Nonlin:2
0011110000011101  Nonlin:2    Inverse Nonlin:4
```

Figure 5 Properties of Random S-box (Continued . . .)

```
COMPLETENESS METRICS
--------------------
              S-BOX                Order           INVERSE S-BOX
   1        2        3        4          1        2        3        4
-------------------------------------------------------------------------
0.000000 0.000000 1.219361 3.000000 --- 0.000000 0.000000 1.156861 3.000000
0.000000 0.250000 1.183572 3.000000 --- 0.000000 0.250000 1.234680 3.000000
0.000000 0.000000 1.125000 3.000000 --- 0.000000 0.250000 1.266541 3.000000
0.000000 0.250000 1.266541 3.000000 --- 0.000000 0.250000 1.183572 3.000000

 INPUT - OUTPUT METRICS
------------------------
         IO INDEPENDENCE          Order         OI INDEPENDENCE
   1        2        3        4          1        2        3        4
-------------------------------------------------------------------------
0.045566 0.177694 0.500000 1.000000 --- 0.034174 0.177694 0.500000 1.000000
0.058572 0.203634 0.500000 1.000000 --- 0.034174 0.094361 0.250000 1.000000
0.022783 0.078634 0.375000 1.000000 --- 0.022783 0.078634 0.375000 1.000000
0.022783 0.161967 0.500000 1.000000 --- 0.058572 0.203634 0.500000 1.000000

 DYNAMIC INPUT - OUTPUT METRICS
--------------------------------
        DYN IO INDEPENDENCE        Order       DYN OI INDEPENDENCE
   1        2        3        4          1        2        3        4
-------------------------------------------------------------------------
0.002820 0.020966 0.059213 0.133271 --- 0.002115 0.020966 0.059213 0.133271
0.012096 0.033804 0.068362 0.133271 --- 0.002115 0.005650 0.011391 0.290132
0.001410 0.004709 0.034578 0.133271 --- 0.001410 0.004709 0.072456 0.290132
0.001410 0.044809 0.133521 0.290132 --- 0.012096 0.033804 0.068362 0.133271

DYNAMIC OUTPUT - OUTPUT METRICS
--------------------------------
     S-BOX DYN OO INDEP    Order    INVS S-BOX DYN OO INDEP
   1        2        3              1        2        3
-------------------------------------------------------------
0.318081 0.624428 0.827975 --- 0.334970 0.647912 0.794066
```

Figure 5 Properties of Random S-box

```
S-BOX vectors
-------------
1111000010011001  Nonlin:4    Inverse Nonlin:4
1011111000010100  Nonlin:4    Inverse Nonlin:4
0010011100011011  Nonlin:4    Inverse Nonlin:4
0101001100110101  Nonlin:4    Inverse Nonlin:4

COMPLETENESS METRICS
--------------------
              S-BOX                Order           INVERSE S-BOX
   1        2        3        4          1        2        3        4
-------------------------------------------------------------------------
0.000000 0.416667 1.125000 3.000000 --- 0.000000 0.333333 1.297180 3.000000
0.000000 0.416667 1.125000 3.000000 --- 0.000000 0.250000 1.250000 3.000000
0.000000 0.166667 1.250000 3.000000 --- 0.250000 0.666667 1.500000 3.000000
0.000000 0.166667 1.250000 3.000000 --- 0.000000 0.416667 1.125000 3.000000
```

Figure 6 Properties of Webster S-box (Continued . . .)

```
 INPUT - OUTPUT METRICS
------------------------
          IO INDEPENDENCE           Order          OI INDEPENDENCE
    1         2         3         4            1         2         3         4
-------------------------------------------------------------------------------
0.047180 0.177694 0.500000 1.000000 --- 0.047180 0.146241 0.375000 1.000000
0.047180 0.177694 0.500000 1.000000 --- 0.094361 0.240602 0.500000 1.000000
0.094361 0.209148 0.500000 1.000000 --- 0.094361 0.312907 0.625000 1.000000
0.094361 0.209148 0.500000 1.000000 --- 0.047180 0.177694 0.500000 1.000000

 DYNAMIC INPUT - OUTPUT METRICS
--------------------------------
         DYN IO INDEPENDENCE         Order        DYN OI INDEPENDENCE
    1         2         3         4            1         2         3         4
-------------------------------------------------------------------------------
0.011391 0.038510 0.094361 0.250000 --- 0.011391 0.030915 0.070771 0.250000
0.011391 0.038510 0.094361 0.250000 --- 0.022783 0.053698 0.094361 0.250000
0.022783 0.046104 0.094361 0.250000 --- 0.022783 0.062369 0.133271 0.250000
0.022783 0.046104 0.094361 0.250000 --- 0.011391 0.038510 0.094361 0.250000

DYNAMIC OUTPUT - OUTPUT METRICS
--------------------------------
     S-BOX DYN OO INDEP    Order    INVS S-BOX DYN OO INDEP
    1         2         3            1         2         3
-------------------------------------------------------------
0.333333 0.550000 0.850000 --- 0.333333 0.400000 1.000000
```

Figure 6 Properties of Webster S-box

```
S-BOX vectors
-------------
1010011101010100  Nonlin:4    Inverse Nonlin:2
1110010000111001  Nonlin:4    Inverse Nonlin:2
1000111011100001  Nonlin:4    Inverse Nonlin:4
0011011010001101  Nonlin:4    Inverse Nonlin:2

COMPLETENESS METRICS
--------------------
               S-BOX                Order           INVERSE S-BOX
    1         2         3         4            1         2         3         4
-------------------------------------------------------------------------------
0.000000 0.083333 1.172180 3.000000 --- 0.000000 0.250000 1.266541 3.000000
0.000000 0.166667 1.117951 3.000000 --- 0.000000 0.250000 1.402933 3.000000
0.000000 0.166667 1.141541 3.000000 --- 0.000000 0.083333 1.172180 3.000000
0.000000 0.166667 1.117951 3.000000 --- 0.000000 0.250000 1.402933 3.000000

 INPUT - OUTPUT METRICS
------------------------
          IO INDEPENDENCE           Order          OI INDEPENDENCE
    1         2         3         4            1         2         3         4
-------------------------------------------------------------------------------
0.022783 0.120301 0.437500 1.000000 --- 0.022783 0.078634 0.375000 1.000000
0.011391 0.078634 0.375000 1.000000 --- 0.011391 0.047180 0.312500 1.000000
0.022783 0.110088 0.375000 1.000000 --- 0.022783 0.120301 0.437500 1.000000
0.011391 0.078634 0.375000 1.000000 --- 0.011391 0.047180 0.187500 1.000000
```

Figure 7 Properties of DES S-box (Continued . . .)

```
 DYNAMIC INPUT - OUTPUT METRICS
---------------------------------
        DYN IO INDEPENDENCE          Order       DYN OI INDEPENDENCE
    1        2        3        4            1        2        3        4
-------------------------------------------------------------------------------
0.001410 0.012367 0.047620 0.133271 --- 0.001410 0.004709 0.072456 0.290132
0.000705 0.010419 0.043727 0.133271 --- 0.000705 0.002825 0.069608 0.290132
0.001410 0.012303 0.034578 0.133271 --- 0.001410 0.012367 0.047620 0.133271
0.000705 0.010419 0.043727 0.133271 --- 0.000705 0.002825 0.008544 0.290132

DYNAMIC OUTPUT - OUTPUT METRICS
-------------------------------
     S-BOX DYN OO INDEP    Order    INVS S-BOX DYN OO INDEP
    1        2        3             1        2        3
-----------------------------------------------------------
0.271739 0.604401 0.829044 --- 0.336366 0.600914 0.783518
```

Figure 7 Properties of DES S-box

```
S-BOX vectors
-------------
0001100111101001  Nonlin:4    Inverse Nonlin:4
1101000110100110  Nonlin:4    Inverse Nonlin:4
1010100100111100  Nonlin:4    Inverse Nonlin:4
1001001101011010  Nonlin:4    Inverse Nonlin:4

COMPLETENESS METRICS
--------------------
               S-BOX                Order          INVERSE S-BOX
    1        2        3        4            1        2        3        4
-------------------------------------------------------------------------------
0.000000 0.166667 1.117951 3.000000 --- 0.000000 0.166667 1.117951 3.000000
0.000000 0.166667 1.117951 3.000000 --- 0.000000 0.166667 1.117951 3.000000
0.000000 0.166667 1.117951 3.000000 --- 0.000000 0.166667 1.117951 3.000000
0.000000 0.166667 1.117951 3.000000 --- 0.000000 0.166667 1.117951 3.000000

 INPUT - OUTPUT METRICS
-------------------------
          IO INDEPENDENCE          Order          OI INDEPENDENCE
    1        2        3        4            1        2        3        4
-------------------------------------------------------------------------------
0.011391 0.078634 0.375000 1.000000 --- 0.011391 0.078634 0.375000 1.000000
0.011391 0.078634 0.375000 1.000000 --- 0.011391 0.078634 0.375000 1.000000
0.011391 0.078634 0.375000 1.000000 --- 0.011391 0.078634 0.375000 1.000000
0.011391 0.078634 0.375000 1.000000 --- 0.011391 0.078634 0.375000 1.000000

 DYNAMIC INPUT - OUTPUT METRICS
---------------------------------
        DYN IO INDEPENDENCE          Order       DYN OI INDEPENDENCE
    1        2        3        4            1        2        3        4
-------------------------------------------------------------------------------
0.000705 0.010419 0.043727 0.133271 --- 0.000705 0.010419 0.043727 0.133271
0.000705 0.010419 0.043727 0.133271 --- 0.000705 0.010419 0.043727 0.133271
0.000705 0.010419 0.043727 0.133271 --- 0.000705 0.010419 0.043727 0.133271
0.000705 0.010419 0.043727 0.133271 --- 0.000705 0.010419 0.043727 0.133271
```

Figure 8 Properties of New S-box (Continued . . .)

```
DYNAMIC OUTPUT - OUTPUT METRICS
-------------------------------
     S-BOX DYN OO INDEP    Order    INVS S-BOX DYN OO INDEP
    1         2         3             1         2         3
-------------------------------------------------------------
0.198651 0.500727 0.735700 --- 0.198651 0.500727 0.735700
```

Figure 8 Properties of New S-box

Conclusions

In this paper we introduced the static and dynamic views of an S-box and used these abstractions to define the properties of an Ideal S-box based on information theoretic ideas. We then presented a new set of design criteria for S-boxes based on the properties of an Ideal S-box. We then demonstrated the usefulness of the new design framework by using it to analyze the S-boxes of DES and to create new S-boxes of various sizes. The new set of design criteria should be a valuable tool that can be used to create S-boxes for cryptosystems of the future.

Bibliography

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," in *CRYPTO 90 Abstracts*, pp. 1–19, August, 1990.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.

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

[4] H. Feistel, W. Notz, and J. L. Smith, "Some crytptographic techniques for machine-to-machine data communications," in *Proceedins of the IEEE*, vol. 63, pp. 1545–1554, 1975.

[5] B. den Boer, "Crptanalysis of F. E. A. L.," in *Advances in Cryptology: Proc. of EUROCRYPT 88*, pp. 167–173, Springer-Verlag, 1989.

[6] W. Fumy, "On the F-function of FEAL," in *Advances in Cryptology:Proc. of CRYPTO 87*, pp. 434–437, Springer-Verlag, 1988.

[7] National Bureau of Standards (U.S.), "Data Encryption Standard (DES)," Tech. Rep. Publication 46, Federal Information Processing Standards, 1977.

[8] M. E. Hellman and et. al., "Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard," tech. rep., Information Systems Laboratory, Stanford University, November, 1976.

[9] A. Shamir, "On the security of DES," in *Advances in Cryptology. Proc. of CRYPTO 85*, pp. 280–281, Springer-Verlag, 1986.

[10]E. F. Brickell, J. H. Moore, and M. R. Purtill, "Structure in the S-boxes of the DES(extended abstract)," in *Advances in Cryptology: Proc. of CRYPTO 86*, pp. 3–8, Springer-Verlag, 1986.

[11]R. Forré, "Methods and instruments for designing S-boxes," *Journal of Crytology*, vol. 2, no. 3, pp. 115–130, 1990.

[12]J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cyptosystem design," in *IEE proceedings, Part E: Computers and Digital Techniques*, vol. 135, pp. 325–335, 1988.

[13]J. B. Kam and G. I. Davida, "Structured design of substituion-permutation encryption networks," *IEEE Transactions on Computers*, vol. C-28, pp. 747–753, 1979.

[14]A. F. Webster, "Plaintext/ciphertext bit dependencies in cryptographic systems," Master's thesis, Queen's University, 1985.

[15]B. Preneel, W. VanLeewijck, L. VanLinden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of boolean functions," in *EUROCRYPT 90 — Abstracts*, pp. 155–165, 1990.

[16]S. Lloyd, "Properties of binary functions," in *EUROCRYPT 90 — Abstracts*, pp. 126–135, 1990.

[17]C. M. Adams and S. E. Tavares, "The structured design of cryptographically good S-boxes," *Journal of Cryptology*, vol. 3, pp. 27–41, 1990.

[18]A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Advances in Cryptology:Proc. of CRYPTO 85*, (New York), pp. 523–534, Springer-Verlag, 1986.

[19]M. H. Dawson, "A unified framework for Substitution box design based on information theory," Master's thesis, Department of Electrical Engineering, Queens University, April 1991.

[20]M. H. Dawson, "An implementation of the algorithms required to measure the information theoretic properties of an S-box and the algorithms to use these measures to create new S-boxes," tech. rep., Department of Electrical Engineering, Queen's University, Feb. 1991.