Information Leakage of a Randomly Selected Boolean Function

A. M. Youssef and S. E. Tavares

Department Of Electrical and Computer Engineering
Queen's University
Kingston, Ontario, Canada, K7L 3N6
email : tavares@ee.queensu.ca

Abstract. It is argued that a boolean function $f : Z_2^n \rightarrow Z_2^m$ is resistant to statistical analysis if there is no significant static and dynamic leakage between its inputs and outputs. In this paper, we derive expressions for the expected value of the information leakage of randomly selected boolean functions and for the interesting cases of randomly selected balanced, and randomly selected injective boolean functions. It is shown that the expected value of different forms of information leakage decreases dramatically with the number of input variables n. For example, for a single output boolean function, we show that the expected value of different forms of leakage goes down exponentially with n.

1 Introduction

Several cryptographic criteria have been previously proposed as a measure of the strength of cryptographic functions. Among these criteria are balance, correlation immunity[18], resiliency[4], nonlinearity[12], Strict Avalanche Criterion (SAC)[21], higher order SAC[7], Propagation Criterion (PC), higher order PC[14], Bit Independence Criterion [20], and Completeness[10].

The above set of cryptographic criteria are not independent of each other and a cryptographic function that satisfies all these criteria would be a golden one. Unfortunately, it can be proven that no function can satisfy all the above set of criteria simultaneously. This can be considered as the main motive for proposing a new set of criteria based on information theory.

Several design criteria, based on information theory, have been proposed in [6],[8], [19], and [24].

In [24] Information leakage was proposed as a measure of the performance of cryptographic functions. Information Leakage can be classified into two classes: Static information leakage and dynamic information leakage. It is argued in [24] that a boolean function is resistant to statistical analysis (e.g., differential cryptanalysis [2], linear cryptanalysis [11], and Siegenthaler's correlation attack [17]) if there is no significant static and dynamic information leakage between its inputs and outputs. In [22], the authors studied the relation between the spectral properties and information leakage of multi-output boolean functions.

Gordon and Retkin [9] conjectured that good substitution boxes (S-boxes) may be built by choosing a random reversible mapping of sufficient size. Their argument is based on the observation that the probability of accidental linearity occurring in such S-boxes decreases dramatically as the size of the S-box increases. Here in this paper, we provide further evidence that bigger S-boxes (by bigger we mean S-boxes with a larger number of inputs) are better by showing that the expected value of information leakage of a randomly selected boolean function decreases rapidly with the number of input variables.

It is worth noting that Brynielsson[3] gives an approximate expression for the expected value of the mutual information between the output and input subvectors for multi-output boolean functions. Here we follow the definition of information leakage given in [24] and give an exact expression for the expected value of different forms of these information leakages for a randomly selected multi-output boolean function and for some other combinatorial structures of interest such as regular mappings, and injective mappings.

2 Definitions

Throughout this paper, let Y be the output of a boolean function $f : \mathrm{Z}_2^n \rightarrow \mathrm{Z}_2^m$, then we have:

Static Information Leakage: the static information leakage of Y, given input subvector $X_k \in \mathrm{Z}_2^k$ (i.e., given that we know k bits of the n-bit input vector) , is defined by

$$SL(Y|X_k) = m - H(Y|X_k), \tag{1}$$

where $H(Y \mid X_k)$ is the conditional entropy of Y given X_k.

Remark: It is easy to show that

$$SL(Y|X_k) = m - H(Y) + I(Y; X_k), \tag{2}$$

where $I(Y; X_k)$ is the mutual information between Y and X_k. Note that if the mutual information $I(Y; X_k)$ is used to define the static information leakage, then the minimum of $I(Y; X_k)$ can be achieved while $H(Y) = 0$ which contradicts our objective. For a good general reference for information theory, see [5].

Dynamic Information Leakage: the dynamic information leakage of ΔY, given the input change vector ΔX is defined by:

$$DL(\Delta Y|\Delta X) = m - H(\Delta Y|\Delta X), \tag{3}$$

where $\Delta Y = Y(X) \oplus Y(X \oplus \Delta X)$.

The self static information leakage of Y is defined as:

$$SSL(Y) = m - H(Y). \tag{4}$$

It is clear that $SSL(Y) = SL(Y \mid X_0)$. We note that the static information leakage $SL(Y \mid X_k) = 0$ is achieved by k^{th} order resilient functions (see [4], [18] for the definition and properties of resilient functions), while zero dynamic information leakage

for all values of $\Delta X \neq 0$ is achieved only by perfect nonlinear functions (see [13], [16] for the definition and properties of both bent and perfect nonlinear functions).

Let Y be the output of a boolean function $f(X)$ and define

$$\begin{aligned} N_y &= \#\{X \in Z_2^n | f(X) = y\}, \\ N_{\dot{x}y} &= \#\{X \in Z_2^n \mid X_k = \dot{x}, Y = y\}, \\ N_{\Delta x \Delta y} &= \#\{X \in Z_2^n \mid f(X \oplus \Delta x) \oplus f(X) = \Delta y\}, \end{aligned} \tag{5}$$

where $\dot{x} \in Z_2^k$, $\Delta x \in Z_2^n$, $y \in Z_2^m$, $\Delta y \in Z_2^m$.
Assuming that all input vectors are equally probable, we have:

$$\begin{aligned} SSL(Y) &= m - \sum_{y \in Z_2^m} \frac{N_y}{2^n} log_2\left(\frac{2^n}{N_y}\right), \\ SL(Y \mid X_k) &= m - 2^{-k} \sum_{\substack{y \in Z_2^m \\ \dot{x} \in Z_2^k}} \frac{N_{\dot{x}y}}{2^{n-k}} log_2\left(\frac{2^{n-k}}{N_{\dot{x}y}}\right), \\ DL(\Delta Y \mid \Delta X) &= m - 2^{-n} \sum_{\substack{\Delta x \in Z_2^n \\ \Delta y \in Z_2^m}} \left(\frac{N_{\Delta x \Delta y}}{2^n}\right) log_2\left(\frac{2^n}{N_{\Delta x \Delta y}}\right). \end{aligned} \tag{6}$$

The problem of finding the expected values of the above forms of information leakage is now reduced to finding the marginal probability distribution of the random variables $N_y, N_{\dot{x}y}, N_{\Delta x \Delta y}$.

3 Information Leakage Of a Randomly Selected Boolean Function

Lemma 3.1:
Let Y be the output of a randomly selected boolean function $f : Z_2^n \rightarrow Z_2^m$ then we have the following probabilities:

$$\begin{aligned} P(N_y = i) &= \binom{2^n}{i} \left(\frac{1}{2^m}\right)^i \left(1 - \frac{1}{2^m}\right)^{2^n - i}, \\ P(N_{\dot{x}y} = i) &= \binom{2^{n-k}}{i} \left(\frac{1}{2^m}\right)^i \left(1 - \frac{1}{2^m}\right)^{2^{n-k} - i}, \\ P(N_{\Delta x \Delta y} = 2i) &= \binom{2^{n-1}}{i} \left(\frac{1}{2^m}\right)^i \left(1 - \frac{1}{2^m}\right)^{2^{n-1} - i}, \Delta x \neq \underline{0}. \end{aligned} \tag{7}$$

Proof: The proof of the above Lemma follows by noting that N_y, $N_{\dot{x}y}$, and $N_{\Delta x \Delta y}/2$ follow the multi-nomial distribution. □

Theorem 3.1:

The expected values of the static and dynamic information leakage of a randomly selected boolean function $f : Z_2^n \rightarrow Z_2^m$ are given respectively by

$$\begin{aligned} \overline{SL(Y \mid X_k)} &= m - 2^m \sum_{i=0}^{2^{n-k}} P(N_{\hat{x}y} = i) \left(\frac{i}{2^{n-k}}\right) log_2\left(\frac{2^{n-k}}{i}\right), \quad 0 \leq k \leq n, \\ \overline{DL(\Delta Y \mid \Delta X)} &= m - \frac{2^m(2^n-1)}{2^n} \sum_{i=0}^{2^{n-1}} P(N_{\Delta x \Delta y} = 2i) \left(\frac{i}{2^{n-1}}\right) log_2\left(\frac{2^{n-1}}{i}\right). \end{aligned} \tag{8}$$

Proof: Theorem 3.1 follows directly from the definition of the expected value, and (for part 2) by noting that $\Delta Y = 0$ for $\Delta X = 0$, and hence $H(\Delta Y \mid 0) = 0$. □

Figs. 1 and 2 show the expected value of the self static information leakage and the expected value of the static leakage given that half the input bits are known. From these graphs , it is clear that the relative dimensions of the boolean functions (i.e., the ratio between n, m) greatly affect different forms of information leakage.

Based on the results above, one can not conclude that S-boxes with $n > m$ are better than S-boxes with $n < m$ because of the method we used in the normalization step (dividing by the number of output bits to get information leakage per output bit). Moreover, S-boxes with $n < m$ provide better diffusion characteristics, and may be used in SPNs with no permutation layers [1] which leads to faster software implementation. The conclusion that we can make at this time is that all forms of information leakage seem to decrease with the number of input variables.

Using theorem 3.1, one can derive an upper bound for the information leakage of a single output boolean function. Single output functions are of practical interest especially for the combining functions in stream ciphers.

Corollary 3.1

Let Y be the output of a single output boolean function, then the expected values of both the static leakage and dynamic leakage are bounded by

$$\begin{aligned} \overline{SL(Y \mid X_k)} &\leq \frac{1}{2^{n-k}}, \qquad 0 \leq k \leq n, \\ \overline{DL(\Delta Y \mid \Delta X)} &\leq \frac{3}{2^n}. \end{aligned} \tag{9}$$

Proof: The above corollary follows by direct substitution into theorem 3.1 and by noting that for the binary entropy function

$$h(t) = -t\ log_2(t) - (1-t) log_2(1-t), \tag{10}$$

we have

$$h(t) \geq 4t - 4t^2, \qquad 1 \geq t \geq 0 \ . \tag{11}$$

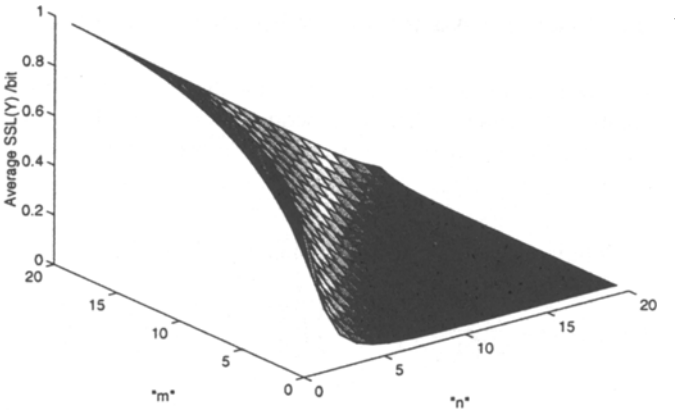

Figure 1 Expected value of $SSL(Y)$

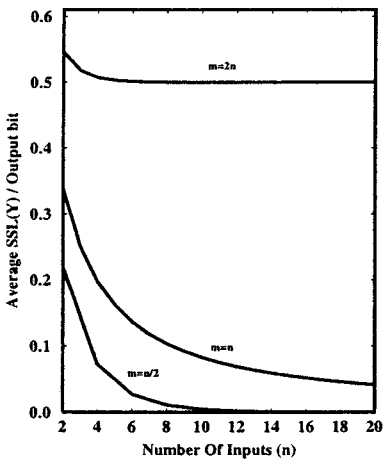

Figure 2(a) Expected Value of $SSL(Y)$

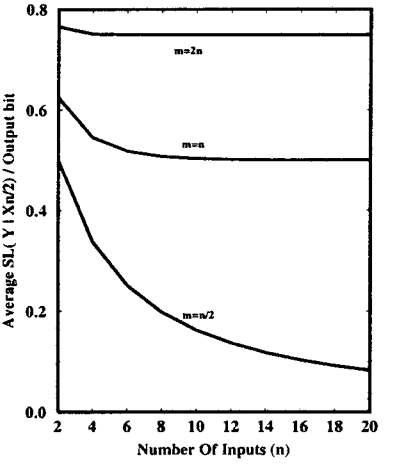

Figure 2(b) Expected Value of $SL(Y \mid X_{n/2})$

4 Information Leakage Of a Randomly Selected Balanced Boolean Function

In this section, we calculate the expected values of both the dynamic leakage and the static leakage for regular (also called balanced) functions. For balanced functions, every output symbol appears an equal number of times as the input varies through all possible values.

Lemma 4.1

Let Y be a randomly selected balanced function $f: \mathrm{Z}_2^n \rightarrow \mathrm{Z}_2^m$, $n \geq m$, then we have

$$P(N_{\dot{x}y} = i) = \frac{1}{B(n,m)} \binom{2^{n-k}}{i} \binom{2^n - 2^{n-k}}{2^{n-m} - i} \frac{(2^n - 2^{n-m})!}{(2^{n-m}!)^{(2^m-1)}} , \qquad (12)$$

where $B(n,m) = \frac{2^n!}{(2^{n-m}!)^{2^m}}$ is the number of $n \times m$ balanced boolean functions.

Proof: For $n \times m$ balanced boolean functions, we have $N_y = 2^{n-m}$. If we fix k input variables, then there are $\binom{2^{n-k}}{i}\binom{2^n-2^{n-k}}{2^{n-m}-i}$ ways of arranging the output such that $Y = y$ when $X_k = \dot{x}$ for i times. The remaining $(2^n - 2^{n-m})$outputs , of which there are only $(2^{n-m} - 1)$ distinct ones, can be permuted in $\frac{(2^n-2^{n-m})!}{(2^{n-m}!)^{(2^m-1)}}$ ways. □

Corollary 4.1

Let Y be a randomly selected bijective mapping $\pi: \mathrm{Z}_2^n \rightarrow \mathrm{Z}_2^n$ then the expected value of the static information leakage of Y given the input subvector X_k, $0 \leq k \leq n$, is given by

$$\overline{SL(Y \mid X_k)} = k. \qquad (13)$$

Proof: The proof follows directly by substituting (12), with $n = m$, into (8). A simpler proof (independent of Lemma 4.1) follows by noting that for any arbitrary bijective function, $\pi: \mathrm{Z}_2^n \rightarrow \mathrm{Z}_2^n$, if we fix k input bits, we will have 2^{n-k} different output symbols with $H(Y \mid X_k) = n - k$. □

In Lemmas 4.2, 4.3, and 4.4 we will derive an expression for the marginal probability density function of the random variable $N_{\Delta x \Delta y}$ for a randomly selected balanced boolean function.

Let

$$G(k_1, k_2, ..., k_{2^{m-1}}) = C(k; k_1, k_2, ..., k_{2^{m-1}}) C(2^n - 2k; l_1, l_1, l_2, l_2, ..., l_{2^{m-1}}, l_{2^{m-1}}) , \qquad (14)$$

where $C(k; k_1, k_2, ..., k_{2^{m-1}}) = \frac{k!}{k_1!\, k_2! \cdots k_{2^{m-1}}!}$, and $l_i = 2^{n-m} - k_i$, $l_i \geq 0$, $k_i \geq 0$, then we have:

Lemma 4.2

The number of balanced functions with $N_{\Delta x \Delta y} \geq 2k,\ \Delta x \neq 0, \Delta y \neq 0$, is upper bounded by

$$\Psi_{n,m}(k) = \binom{2^{n-1}}{k} 2^k \sum_{\sum k_i = k} G(k_1, k_2, ..., k_{2^{m-1}}) \ , \tag{15}$$

where $G(k_1, k_2, ..., k_{2^{m-1}})$ is given by (14).

Proof: By noting that we have 2^m distinct output symbols, and each of them is repeated 2^{n-m} times, it is easy to see that for a given $\Delta y \neq 0, \Delta x \neq 0$ we have 2^{m-1} distinct XOR pairs, each of them is repeated 2^{n-m} times. Group each of these 2^{n-m} pairs into one set.

There is only one way to choose k_i pairs from the set $s, s = 1, 2, ..., 2^{m-1}$ (as the pairs within a given set are indistinguishable). These k pairs can be permuted in $C(k; k_1, k_2, ..., k_{2^{m-1}})$ ways. The remaining $2^n - 2k$ output symbols can be permuted into $C(2^n - 2k; l_1, l_1, l_2, l_2, ..., l_{2^{m-1}}, l_{2^{m-1}})$ ways, where $l_i = 2^{n-m} - k_i$. Note that there are two possible orders for each pair, giving 2^k total possible orders, and $\binom{2^{n-1}}{k}$ possible choices for the X positions of these k pairs.

The construction approach described above does not guarantee that these balanced functions are all distinct, and so $\Psi_{n,m}(k)$ is an upper bound. □

Let

$$D(k_1, k_2, ..., k_{2^{m-1}}) = C(k; k_1, k_2, ..., k_{2^m}) C(2^n - 2k; l_1, l_2, ..., l_{2^m}) \ , \tag{16}$$

and $l_i = 2^{n-m} - 2k_i,\ l_i \geq 0,\ k_i \geq 0$ then we have:

Lemma 4.3

The number of balanced functions with $N_{\Delta x 0} \geq 2k, \Delta x \neq 0, \Delta y = 0$, is upper bounded by

$$\Phi_{n,m}(k) = \binom{2^{n-1}}{k} \sum_{\sum k_i = k} D(k_1, k_2, ..., k_{2^m}) \ , \tag{17}$$

where $D(k_1, k_2, ..., k_{2^m})$ is given by (16).

Proof: Similar to the proof of Lemma 4.2. □

Lemma 4.4

The exact number of balanced functions with $N_{\Delta x \Delta y} = 2k, \Delta x \neq 0, \Delta y \neq 0$,, and the exact number of balanced functions with $N_{\Delta x \Delta y} = 2k, \Delta x \neq 0, \Delta y = 0$, are given respectively by

$$\Lambda_{n,m,\Delta y}(k) = \sum_{i=k}^{2^{n-1}} (-1)^{i-k} \binom{i}{k} \Psi_{n,m}(i) \,,$$
$$\Lambda_{n,m,0}(k) = \sum_{i=k}^{2^{n-1}} (-1)^{i-k} \binom{i}{k} \Phi_{n,m}(i) \,. \tag{18}$$

Proof: Follows by using the inclusion-exclusion principle [15]. □

By direct substitution, the expected value of the dynamic leakage of a randomly selected balanced function is given by

Theorem 4.1

$$\begin{aligned}\overline{DL(\Delta Y \mid \Delta X)} = m \\ - \frac{(2^n-1)(2^m-1)}{2^n} \sum_{i=0}^{2^{n-1}} \frac{\Lambda_{n,m,\Delta y}(i)}{B(n,m)} \left(\frac{i}{2^{n-1}}\right) log_2\left(\frac{2^{n-1}}{i}\right) \\ - \frac{(2^n-1)}{2^n} \sum_{i=0}^{2^{n-1}} \frac{\Lambda_{n,m,0}(i)}{B(n,m)} \left(\frac{i}{2^{n-1}}\right) log_2\left(\frac{2^{n-1}}{i}\right).\end{aligned} \tag{19}$$

Corollary 4.2

Let Y be a randomly selected bijective mapping $\pi : \ Z_2^n \rightarrow Z_2^n$ then the expected value of the dynamic information leakage given the input change vector ΔX, is given by

$$\overline{DL(\Delta Y \mid \Delta X)} = n - \frac{(2^n-1)^2}{2^n} \sum_{i=0}^{2^{n-1}} \frac{\Lambda_{n,n,\Delta y}(i)}{n!} \left(\frac{i}{2^{n-1}}\right) log_2\left(\frac{2^{n-1}}{i}\right). \tag{20}$$

where $\Lambda_{n,n,\Delta y}$ is given by (18).

Proof: Corollary 4.2 is a special case (with $n = m$) of theorem 4.1. □

Remark: Note that $\Lambda_{n,n,0} = 0$ as each output symbol occurs once. Note also that, by substitution into (15) with $n = m$, $\Psi_{n,n}$ can be simplified to

$$\Psi_{n,n}(i) = \binom{2^{n-1}}{i}^2 i! \ 2^i \ (2^n - 2i)! \tag{21}$$

Fig.3 shows a comparison between the expected value of dynamic information leakage of a randomly chosen $n \times n$ bijective mapping and that of a randomly chosen function of the same dimensions.

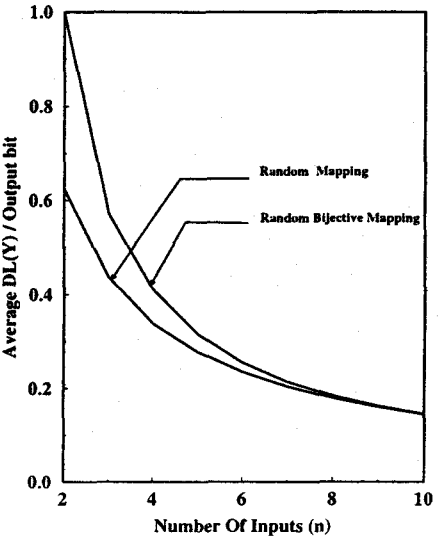

Figure 3 Expected value of $DL(Y)$ for an $n \times n$ random mapping and an $n \times n$ random bijective mapping

5 Information Leakage Of a Randomly Selected Injective Boolean Function

In this section, we calculate the expected values of both the dynamic leakage and the static leakage for injective functions.

Theorem 5.1

Let Y be the output of a randomly selected injective function $f : Z_2^n \rightarrow Z_2^m$, $n \leq m$, then

$$\overline{SL(Y \mid X_k)} = (m - n) + k. \tag{22}$$

Proof: The theorem follows by noting that for any arbitrary injective function, $f : Z_2^n \rightarrow Z_2^m$, if we fix k input bits, we will have 2^{n-k} different output symbols with $H(Y \mid X_k) = n - k$. □

Lemma 5.1

The number of injective functions with $N_{\Delta x \Delta y} \geq 2k, \Delta x \neq 0, \Delta y \neq 0$, is upper bounded by

$$\Psi_{n,m}(k) = \binom{2^{n-1}}{k} \binom{2^{m-1}}{k} 2^k \; In(2^m - 2k, 2^n - 2k) \tag{23}$$

where

$$In(u,v) = \prod_{i=0}^{(v-1)} (u-i). \tag{24}$$

Proof: Lemma 5.1 follows by using an argument similar to that used to prove Lemma 4.2. □

Lemma 5.2

The exact number of injective functions with $N_{\Delta x \Delta y} = 2k, \Delta x \neq 0, \Delta y \neq 0$, is given by

$$\Lambda_{n,m,\Delta y}(k) = \sum_{i=k}^{2^{n-1}} (-1)^{i-k} \binom{i}{k} \Psi_{n,m}(i) \; . \tag{25}$$

Remark: Note that $N_{\Delta x\, 0} = 0$ for $\Delta x \neq 0$, and hence $\Lambda_{n,m,0} = 0$.

Theorem 5.2

$$\overline{DL(\Delta Y; \Delta X)} = m - \frac{(2^n-1)(2^m-1)}{2^n} \sum_{i=0}^{2^{n-1}} \frac{\Lambda_{n,m,\Delta y}(i)}{In(2^m,2^n)} \left(\frac{i}{2^{n-1}}\right) log_2\left(\frac{2^{n-1}}{i}\right), \tag{26}$$

where $In(2^m, 2^n)$, the number of $n \times m$ injective boolean functions, is given by (24).

Numerical substitution into the theorem 5.2 shows that the dynamic information leakage of a randomly selected injective function decreases with the number of input variables. This rate of decrease is very similar to that of a randomly selected boolean function with the same number of inputs and outputs, especially for $n \lll m$. This can be explained by noting that for $n \lll m$, a randomly selected function is most likely to be injective.

6 Conclusion

Many of the previously known cryptographic criteria are related to information leakage. Most of these criteria require zero information leakage in some domain. However, they often constrain the function to such an extent that large information leakage of other types become likely. These leakages provide useful information for the cryptanalyst to develop attacks on the cipher. This motivates the minimization of information leakage as a general criterion for cryptographic functions.

We have derived expressions for the expected values of the static and dynamic information leakage of randomly selected boolean functions and for randomly selected balanced, and injective boolean functions. Based on this we showed that the expected values of the information leakages decrease dramatically with the number of input variables. In some cases, we showed that this decrease is exponential. With the same approach developed in this paper, one can show that the variance of different forms of information leakage also decreases dramatically with the number of input variables. Using an approach similar

to the one developed in [23] one can also show that the expected maximum value of different forms of information leakage decrease with the number of input variables. This indicates that cryptographically strong boolean functions may be obtained by choosing random mappings of sufficiently large dimensions.

References

1. C.M. Adams. *A Formal and Practical Design Procedure for Substitution-Permutation Network Cryptosystems.* PhD thesis, Queen's University, Kingston, Ontario, Canada, September, 1990.
2. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology, vol. 4, no. 1, pp. 3–72,* 1991.
3. L. Brynielsson. The information leakage through a randomly generated function. *Advances in Cryptology: Proc. of EUROCRYPT '91, Springer-Verlag, Berlin, pp. 552–553,* 1991.
4. B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich, and R. Smolensky. The bit extraction problem or t-resilient functions. *Proc. 26th IEEE Symposium on Foundation of Computer Science, pp. 396–407,* 1985.
5. T.M. Cover and J.A. Thomas. *Elements of Information Theory.* John Wiely & Sons Inc, 1991.
6. M.H. Dawson and S.E. Tavares. An expanded set of S-box design criteria based on information theory and its relation to differential attacks. *Advances in Cryptology: Proc. of EUROCRYPT '91, Springer-Verlag, pp. 352–365,* 1992.
7. R. Forré. The strict avalanche criterion: Spectral properties of boolean functions and an extended definition. *Advances in Cryptology: Proc. of CRYPTO '88, Springer-Verlag, pp. 450–468,* 1989.
8. R. Forré. Methods and instruments for designing S-boxes. *Journal of Cryptology, Vol .2, No.3 pp. 115–130,* 1990.
9. J. Gordon and H. Retkin. Are big S-boxes best ? *Lecture Notes in Computer Science : Proc. of the Workshop on Cryptography, Springer-Verlag, Berlin, pp.257–262,* 1982.
10. J.B. Kam and G.I. Davida. Structured design of substitution-permutation encryption networks. *IEEE Trans. Comp. C-28, pp.747–753,* 1979.
11. M. Matsui. Linear cryptanalysis method for DES cipher. *Advances in Cryptology: Proc. of EUROCRYPT '93, Springer-Verlag, Berlin. pp. 386–397,* 1994.
12. W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. *Advances in Cryptology: Proc. of EUROCRYPT' 89, Springer-Verlag, pp. 549–562,* 1990.
13. K. Nyberg. Perfect nonlinear S-boxes. *Advances in Cryptology: Proc. of EUROCRYPT '91 , Springer-Verlag, pp. 378–386,* 1992.

14. B. Preneel, W.V. Leekwijk, L.V. Linden, R.Govaerts, and J. Vandewalle. Propagation charachteristic of boolean functions. *Advances in Cryptology: Proc. of EUROCRYPT '90, Springer-Verlag, pp. 161–173*, 1991.
15. F.S. Roberts. *Applied Combinatorics*. Englewood Cliffs, N.J.: Prentice-Hall, 1984.
16. O.S Rothaus. On bent functions. *Journal of Combinatorial Theory, Vol. 20(A):300–305*, 1976.
17. T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Trans. Comput., Vol.C-34, No. 1, pp. 81:85*, 1985.
18. T. Siegenthaler. Correlation-immunity of nonlinear combining functions forcryptographic applications. *IEEE Trans. on Inform. Theory, Vol.IT-30, No.5, pp. 776:780*, Sept. 1984.
19. M. Sivabalan, S.E. Tavares, and L.E. Peppard. On the design of SP networks from an information theoretic point of view. *Advances in Cryptology: Proc. of CRYPTO '92, Springer-Verlag, Berlin, pp. 260–279*, 1993.
20. A.F. Webster. Plaintext / ciphertext bit dependencies in cryptographic systems. Master's thesis, Queen's University, Kingston, Ontario, Canada, December, 1985.
21. A.F. Webster and S.E. Tavares. On the design of S-boxes. *Advances in Cryptology : Proc. of CRYPTO '85 , Springer-Verlag, pp. 523–534*, 1986.
22. A.M .Youssef and S.E. Tavares. Spectral properties and information leakage of multi-output boolean functions. *In Proceedings of the IEEE International Symposium On Information Theory. Whistler, B.C., Canada, Sep. 17–22*, 1995.
23. A.M. Youssef, S.E. Tavares, S. Mister, and C.M. Adams. Linear approximation of injective s-boxes. *IEE Electronics Letters, Vol. 31, No. 25, pp.2168-2169*, 1995.
24. M. Zhang, S.E. Tavares, and L.L. Campbell. Information leakage of boolean functions and its relationship to other cryptographic criteria. *Proceedings of 2nd ACM Conference on Computer and Communications Security, Fairfax, Virgina, pp. 156-165.*, 1994.