On the Immunity of S-boxes against Linear Cryptanalysis

Josef Pieprzyk
Chris Charnes
Jennifer Seberry*

Center for Computer Security Research
Department of Computer Science
University of Wollongong
Wollongong, NSW 2500, AUSTRALIA

e-mail: josef@cs.uow.edu.au
charnes@cs.uow.edu.au
jennie@cs.uow.edu.au

Abstract

Recently Matsui announced an attack on the DES algorithm. The attack relies on the approximation of S-boxes by linear functions. To determine the best linear approximation, Matsui defines linear approximation tables (LAT) for S-boxes. In this paper we examine the relation between Matsui's linear approximation tables and the nonlinearities of corresponding S-boxes.

1 Introduction

The recent cryptographic attack introduced by Matsui [2] relies on the approximation of S-boxes by linear functions. For a given S-box, every output or linear combination of outputs can be approximated by linear functions. Matsui showed how to find the best linear approximation for the S-boxes

*Support for this project was provided in part by the Australian Research Council under the reference number A491131885

used in the DES algorithm and how to use this to break the algorithm. However, there appears to be some misunderstanding of the relationship between this attack and the significance of the linear approximation tables (LAT) introduced by Matsui. In this paper we will explain the relation between nonlinearity and linear approximation tables. We prove that linear approximation tables give the nonlinearities of every linear combination of output functions. Hence the design criteria for S-boxes now has to include an extended measure of nonlinearity of S-boxes; in particular this measure must be consistent with the measure introduced by Nyberg in [4]. Some preliminary comments about the influence of linear cryptanalysis on the design of S-boxes can be found in [9].

2 Background

We denote by $x \in \{0,1\}^n = X^n$ a binary string of length n. A Boolean function f is defined as a mapping

$$f : X^n \longrightarrow X.$$

The set of all n-variable linear Boolean functions is

$$L_n = \{f \mid f : X^n \to X; f = a_1x_1 \oplus \ldots \oplus a_nx_n\},$$

where $a_i \in \{0,1\}$ and $x_i \in X$ for $i = 1, \ldots, n$, and $\oplus$ is the Exclusive-OR operation. The set of n-variable affine Boolean functions is

$$A_n = \{f \mid \ell \in L_n; f = \ell \oplus a_0\}$$

where $a_0 \in X$.

A Boolean function $f(x)$ can also be represented in the form of a truth table. This table is described by the following vector

$$f(x) = (f_0, f_1, \ldots, f_{2^n-1}),$$

where f_i is the value of the function $f(\alpha_i)$ and α_i is the binary representation of the integer i; i.e., $i = \sum_{j=1}^{n} 2^{j-1}\alpha_i[j]$ and $\alpha_i = (\alpha_i[1], \ldots, \alpha_i[n])$.

Definition 2.1 *The Hamming distance between two Boolean functions $f, g : X^n \to X$, is defined as*

$$d(f,g) = wt(f_0 \oplus g_0, f_1 \oplus g_1, \ldots, f_{2^n-1} \oplus g_{2^n-1}),$$

where $wt(\alpha)$ is the weight, i.e, the number of ones of the binary string $\alpha \in X^n$.

The nonlinearity of Boolean functions is defined as follows, (see also [1],[3],[4],[6]).

Definition 2.2 *The nonlinearity $\mathcal{N}(f)$ of a Boolean function $f : X^n \to X$ is*

$$\mathcal{N}(f) = \min_{\ell \in A_n} d(\ell, f),$$

i.e., it is the minimal distance between the function f and the set of affine functions.

Nonlinearity can also be expressed in terms of the Walsh transform $\hat{F}(u)$ of f:

$$\mathcal{N}(f) = 2^{n-1} - \max_{u \in X^n} \frac{|\hat{F}(u)|}{2},$$

see [8].

Definition 2.3 *A $(n \times m)$ S-box is a collection of m functions $F_i(x)$, $i = 1, \ldots, m$, in n Boolean variables $x = (x_1, \ldots, x_n)$ for which*

$$S(x) = (F_1(x), \ldots, F_m(x)).$$

The next definition is taken from Matsui's paper [2].

Definition 2.4 *A linear approximation table (LAT) for a S-box $S(x)$ is a $(2^n \times 2^m)$ array of integers where the (α, β)-entry is calculated as follows:*

$$LAT_S(\alpha, \beta) = \#\{x \mid 0 \le x \le 2^n - 1; (\bigoplus_{i=1}^{n}(x[i] \bullet \alpha[i])) = (\bigoplus_{j=1}^{m}(S(x)[j] \bullet \beta[j]))\},$$

where $\bullet$ is the bitwise AND operation, $x = \sum_{i=1}^{n} 2^{i-1} x[i]$, $\alpha = \sum_{i=1}^{n} 2^{i-1}\alpha[i]$, and $\beta = \sum_{j=1}^{m} 2^{j-1}\beta[j]$ (where $x[i], \alpha[i], \beta[j] \in X = \{0, 1\}$).

Definition 2.5 *(Nyberg [4]) The nonlinearity of a $(n \times m)$ S-box $S(x)$ is*

$$\mathcal{N}(S(x)) = \min_{w=(w_1,\ldots,w_m) \in X^m; v \in X} \mathcal{N}(w_1 F_1 \oplus \ldots \oplus w_m F_m \oplus v). \qquad (1)$$

3 Properties of Linear Approximation Tables

Assume that a binary string $\alpha = (\alpha[1], \ldots, \alpha[n])$ generates a linear function $\ell_\alpha(x) \in L_n$ defined as

$$\ell_\alpha(x) = x_1\alpha[1] \oplus \ldots \oplus x_n\alpha[n].$$

Let a binary string $\beta = (\beta[1], \ldots, \beta[m])$ describe a Boolean function $S_\beta(x)$ defined as the linear combination of output functions of a S-box:

$$S_\beta(x) = F_1(x)\beta[1] \oplus \ldots \oplus F_m(x)\beta[m].$$

Lemma 3.1

$$LAT_S(\alpha, \beta) = 2^n - d(\ell_\alpha(x), S_\beta(x)). \tag{2}$$

Proof : The (α, β)-entry of the LAT_S table indicates the number of arguments x for which the values of $\ell_\alpha(x)$ and $S_\beta(x)$ coincide. On the other hand, the distance $d(\ell_\alpha(x), S_\beta(x))$ gives the number of arguments for which the two functions differ. Thus equation (2) holds. □

Lemma 3.2 *For a fixed vector $\beta \in X^n$, the following inequality holds*

$$\forall_{\alpha \in X^n} \mathcal{N}(S_\beta(x)) \leq LAT_S(\alpha, \beta) \leq 2^n - \mathcal{N}(S_\beta(x)). \tag{3}$$

Proof : Note first that the nonlinearity of a function $f(x)$ is defined as

$$\mathcal{N}(f) = \min_{\ell \in A_n} d(\ell, f).$$

An affine function ℓ is either in L_n or in $A_n \setminus L_n$, so

$$\mathcal{N}(f) = \min(\min_{\ell \in L_n} d(\ell, f), \min_{\ell \in A_n \setminus L_n} d(\ell, f))$$

and

$$\mathcal{N}(f) = \min(\min_{\ell \in L_n} d(\ell, f), 2^n - \min_{\ell \in L_n} d(\ell, f)).$$

Consider now the following two bounds: $\min_{\alpha \in X^n} LAT_S(\alpha, \beta)$ and $\max_{\alpha \in X^n} LAT_S(\alpha, \beta)$. ¿From Equation (2) we have

$$\begin{aligned} \min_{\alpha \in X^n} LAT_S(\alpha, \beta) &= \min_{\alpha \in X^n} (2^n - d(\ell_\alpha(x), S_\beta(x))) \\ = 2^n - \max_{\alpha \in X^n} d(\ell_\alpha(x), S_\beta(x)) &\geq \min_{\alpha \in X^n} d(\ell_\alpha(x) \oplus 1, S_\beta(x)) \\ = min_{\ell \in A^n} d(\ell(x), S_\beta(x)) &= \mathcal{N}(S_\beta(x)). \end{aligned}$$

The upper bound is

$$\max_{\alpha \in X^n} LAT_S(\alpha, \beta) = 2^n - \min_{\alpha \in X^n} d(\ell_\alpha(x), S_\beta(x) \leq 2^n - \mathcal{N}(S_\beta(x)).$$

Therefore Equation (3) holds. □

Entries (α, β) specify the closest affine approximation of the function $S_\beta(x)$. If there is a linear function ℓ_{α^*} for which $LAT_S(\alpha^*, \beta) = \mathcal{N}(S_\beta(x))$, then the closest approximation is the linear function ℓ_{α^*}. However, if there is a linear function ℓ_{α^*} for which $LAT_S(\alpha^*, \beta) = 2^n - \mathcal{N}(S_\beta(x))$, then the closest approximation is the affine function $\ell_{\alpha^*} \oplus 1$.

So we have the following theorem.

Theorem 3.1 *For every function $S_\beta(x)$, the best affine approximation is given by either the function $\ell_{\alpha^*}(x)$ if the entry $LAT_S(\alpha^*, \beta) = \mathcal{N}(S_\beta(x))$, or $\ell_{\alpha^*}(x) \oplus 1$ if $LAT_S(\alpha^*, \beta) = 2^n - \mathcal{N}(S_\beta(x))$.*

This theorem has the following corollaries.

Corollary 3.1 *Let $S(x) = (F_1(x), \ldots, F_m(x))$ and β be a combination of functions $F_i(x)$ such that $S_\beta(x)$ is affine, then there is a single $\alpha^* \in L_n$ such that $LAT_S(\alpha^*, \beta) = 0$ or 2^n. The other entries of the table are: $LAT_S(\alpha, \beta) = 2^{n-1}$, if $\alpha \neq \alpha^*$.*

Example: Consider $GF(2^4)$ and the field automorphism $\sigma : x \to x^2$. Since σ is a linear operation, the linear approximation table has the form:

8	8	16	8	8	8	8	8	8	8	8	8	8	8	8
8	8	8	8	8	8	8	8	8	8	8	16	8	8	8
8	8	8	8	8	8	8	8	8	8	8	8	8	8	16
8	16	8	8	8	8	8	8	8	8	8	8	8	8	8
16	8	8	8	8	8	8	8	8	8	8	8	8	8	8
8	8	8	8	8	8	8	8	8	8	8	8	8	16	8
8	8	8	8	8	8	8	8	8	8	8	8	16	8	8
8	8	8	8	8	8	8	16	8	8	8	8	8	8	8
8	8	8	8	8	8	8	8	8	8	16	8	8	8	8
8	8	8	16	8	8	8	8	8	8	8	8	8	8	8
8	8	8	8	8	8	16	8	8	8	8	8	8	8	8
8	8	8	8	8	8	8	8	8	16	8	8	8	8	8
8	8	8	8	8	8	8	8	16	8	8	8	8	8	8
8	8	8	8	8	16	8	8	8	8	8	8	8	8	8
8	8	8	8	16	8	8	8	8	8	8	8	8	8	8

In this example the first column for $\alpha = 0$ and the first row with $\beta = 0$ are omitted. It is easy to see that every function $S_\beta(x)$ can be represented by the complement of a linear function (where the corresponding entry is $2^4 = 16$).

Corollary 3.2 *¿From a given $LAT_S(\alpha, \beta)$, it is possible to recover all the nonlinearities of $S_\beta(x)$ by selecting the minimal and the maximal values from the column $LAT_S(\alpha, \beta)$; $\alpha \in X^n$. Denote these two values by $LAT_S(\alpha_{min}, \beta)$ and $LAT_S(\alpha_{max}, \beta)$. Then the nonlinearity of $S_\beta(x)$ is*

$$\min(LAT_S(\alpha_{min}, \beta), 2^n - LAT_S(\alpha_{max}, \beta)).$$

Corollary 3.3 *The nonlinearity of $S(x)$ is defined as*

$$\mathcal{N}(S(x)) = \min_{\beta \in X^m} \mathcal{N}(S_\beta(X)). \tag{4}$$

Equation (4) is equivalent to the definition of nonlinearity introduced by Nyberg [4]. It characterizes the strength of S-boxes against linear cryptanalysis.

4 Linear Approximation Tables of Permutations

In this section we assume that $m = n$ and $S(x) = (F_1(x), \ldots, F_n(x))$ is a permutation. Therefore $S(x)$ has an inverse: $S^{-1}(x) = (F_1^{-1}(x), \ldots, F_n^{-1}(x))$. The following theorem describes the relation between the linear approximation tables of $S(x)$ and $S^{-1}(x)$.

Theorem 4.1

$$LAT_S(\alpha, \beta) = LAT_{S^{-1}}(\beta, \alpha).$$

Proof : The definition of $LAT_S(\alpha, \beta)$ states that

$$LAT_S(\alpha, \beta) = \#\{x \mid 0 \leq x \leq 2^n - 1; (\bigoplus_{i=1}^{n}(x[i] \bullet \alpha[i])) = (\bigoplus_{j=1}^{n}(S(x)[j] \bullet \beta[j]))\}.$$

Since our S-box is a permutation we can count the number of output values $y = S(x)$ instead of $x = S^{-1}(y)$, this does not change the entries $LAT_S(\alpha, \beta)$. Therefore

$$\begin{aligned} LAT_S(\alpha, \beta) &= \#\{y \mid 0 \leq y \leq 2^n - 1; \\ &\quad (\bigoplus_{i=1}^{n}(S^{-1}(y)[i] \bullet \alpha[i])) = (\bigoplus_{j=1}^{m}(y[j] \bullet \beta[j]))\} \\ &= LAT_{S^{-1}}(\beta, \alpha). \end{aligned}$$

□

Corollary 4.1 *If $\ell_\alpha(x)$ is the best linear approximation of $S_\beta(x)$ then $\ell_\beta(x)$ is the best linear approximation of $S_\alpha^{-1}(x)$.*

There have been several definitions proposed for the nonlinearity of permutations. In earlier work, see [7], the nonlinearity of a permutation was defined as the minimum value of nonlinearities of the components; so

$$\mathcal{N}_{(1)}(S(x)) = \min_{i=1,\ldots,n} \mathcal{N}(F_i(x)),$$

where $S(x) = (F_1(x), \ldots, F_n(x))$.

But as the example below shows there are permutations whose every component is highly nonlinear, and yet some components of the inverse permutation have low nonlinearity.

In view of this it was concluded that the appropriate measure of nonlinearity of permutations should be

$$\mathcal{N}_{(2)}(S(x)) = \min_{i=1,\ldots,n} (\mathcal{N}(F_i(x)), \mathcal{N}(F_i^{-1}(x)),$$

where $S^{-1}(x) = (F_1^{-1}(x), \ldots, F_n^{-1}(x))$ is the inverse of $S(x)$.

Regarding the linear approximation attack of Matsui [2], it is obvious that the nonlinearity of a permutation should be defined using its linear approximation table, or equivalently applying the definition given by Nyberg [4]. Let γ be

$$\gamma = \max_{\alpha,\beta=1,\ldots,2^n-1} \mid LAT_S(\alpha, \beta) - 2^{n-1} \mid,$$

then the nonlinearity of a permutation $S(x)$ is

$$\mathcal{N}(S(x)) = 2^{n-1} - \gamma. \tag{5}$$

It is obvious that the following inequalities hold

$$\mathcal{N}_{(1)}(S(x)) \geq \mathcal{N}_{(2)}(S(x)) \geq \mathcal{N}(S(x)).$$

The nonlinearity $\mathcal{N}(S(x))$ can be obtained from the LAT_S table by selecting the column (indexed by β) which has the the smallest nonlinearity

$$\mathcal{N}(S(x)) = \min_{\beta=1,\ldots,2^n-1} \mathcal{N}(S_\beta(x)). \tag{6}$$

The same value can also be obtained by selecting the row (indexed by α) with the smallest nonlinearity. Hence

$$\mathcal{N}(S^{-1}(x)) = \min_{\alpha=1,\ldots,2^n-1} \mathcal{N}(S_\alpha^{-1}(x)). \tag{7}$$

Compare this result with Theorem 1 of Nyberg [4].

Example: Consider the cubing permutation in $GF(2^4)$. The linear approximation table for this permutation has the following form.

10	10	10	10	10	10	12	8	8	6	8	6	8	6	6
10	6	6	10	10	6	8	8	8	10	12	6	8	10	10
10	10	10	6	6	6	8	8	8	6	8	10	12	10	10
6	6	10	6	10	10	8	8	12	10	8	10	8	6	10
10	6	6	10	10	6	8	8	8	10	12	6	8	10	10
6	10	6	10	6	10	8	12	8	10	8	10	8	10	6
10	6	6	10	10	6	8	8	8	10	12	6	8	10	10
6	10	6	10	6	10	8	12	8	10	8	10	8	10	6
10	10	10	6	6	6	8	8	8	6	8	10	12	10	10
10	10	10	6	6	6	8	8	8	6	8	10	12	10	10
6	6	10	6	10	10	8	8	12	10	8	10	8	6	10
10	10	10	10	10	10	12	8	8	6	8	6	8	6	6
10	10	10	10	10	10	12	8	8	6	8	6	8	6	6
6	10	6	10	6	10	8	12	8	10	8	10	8	10	6
6	6	10	6	10	10	8	8	12	10	8	10	8	6	10

.

As before, the first column for $\alpha = 0$ and the first row with $\beta = 0$ are omitted. The smallest entry is 6 and the largest is 12, so the nonlinearity is $\min(6, 16 - 12) = 4$. All the (α, β)'s with entries 12 give the most effective approximation of $S_\beta(x)$ by the complement of the linear function $\ell_\alpha(x)$.

5 Conclusions

The core of Matsui's [2] linear cryptanalysis is the linear approximation table. We showed that these tables not only give nonlinearity profiles of the output functions, but also characterize the nonlinearities of their linear combinations. In view of Matsui's attack the designers of S-boxes now have to include an additional requirement related to the nonlinearity of S-boxes. The nonlinearity of a S-box is the the smallest nonlinearity of the linear combinations of output functions – this definition of nonlinearity was introduced by Nyberg [4]. To ensure that an encryption algorithm is resistant to linear cryptanalysis, it is necessary to use S-boxes of the highest possible nonlinearity.

Note that linear cryptanalysis fails if all the entries are 2^{n-1}. Thus we should design S-boxes so that their linear approximation tables contain entries close to 2^{n-1}. There are two independent ways of achieving this goal. The first way is to design S-boxes with the highest possible nonlinearity (getting the best design for a fixed size n of the S-box). The second way is to design S-boxes with a large value of n, as nonlinearities increase asymptotically with 2^{n-1}. It turns out that even a random selection of S-boxes, for a large enough parameter n, can generate highly nonlinear S-boxes ([5]).

ACKNOWLEDGMENT

We would like to thank our friends from the Crypto Group for continuing support.

References

[1] C. Adams and S. Tavares. The structured design of cryptographically good S-boxes. *Journal of Cryptology*, 3:27–41, 1990.

[2] M. Matsui. Linear cryptanalysis method for DES cipher. Abstracts of EUROCRYPT'93, May 1993.

[3] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. *Proceedings of EUROCRYPT'89, Lecture Notes in Computer Science, Advances in Cryptology*, 434:549–562, 1989.

[4] K. Nyberg. On the construction of highly nonlinear permutations. In *Extended Abstracts - Eurocrypt'92*, pages 89–94, May 1992.

[5] L.J. O'Connor. An analysis of product ciphers based on the properties of Boolean functions. PhD thesis, the University of Waterloo, 1992. Waterloo, Ontario, Canada.

[6] J. Pieprzyk and G. Finkelstein. Towards effective nonlinear cryptosystem design. *IEE Proceedings-E, Computers and Digital Techniques*, 135(6):325–335, November 1988.

[7] J.P. Pieprzyk. On bent permutations. In *Proceedings of the International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing, Las Vegas*, August 1991.

[8] R.A. Rueppel. *Stream ciphers, in G. Simmons (ed.), Contemporary Cryptology - The Science of Information Integrity.* IEEE Press, New York, 1992.

[9] J. Seberry, X.M. Zhang, and Y. Zheng. Systematic generation of cryptographically robust S-boxes. Proceedings of the 1st ACM Conference on Computer and Communication Security, November 1993.