

Nonlinearity of the Round Function

Marcin Kontak
mkontak@wp.pl

Janusz Szmidt
j.szmidt@poczta.tp.pl

Military University of Technology
Faculty of Cybernetics
Institute of Mathematics and Cryptology
ul. Kaliskiego 2, 00-908 Warsaw, Poland

Abstract

In the paper we present the results which enable to calculate the nonlinearity of round functions with quite large dimensions e.g. 32×32 bits, which are used in some block ciphers. This can be applied to improve the resistance of these ciphers against linear cryptanalysis. The involved method of calculating the nonlinearity is rested on the notion of multi-dimensional Walsh transform. At the end we give the application to linear cryptanalysis of the TGR block cipher.

2000 Mathematics Subject Classification: 94A60.

Keywords: Boolean functions, Walsh transform, nonlinearity, S-boxes, round function.

This work has been supported by the Polish Committee of Scientific Research in years 2003-2006 as the Project 0 T00A 020 25.

1 Introduction

The linear cryptanalysis introduced by Mitsuru Matsui [6] is one of the basis attacks on block ciphers. The resistance of block cipher against this attack is the main requirement in stating its security. The notion of nonlinearity of Boolean functions and Boolean mappings (S-boxes) introduced in [7] and [8, 9] is essential in formulation of linear cryptanalysis. In this paper we consider the round function of a block cipher consisting of parallel S-boxes which inputs are concatenated and outputs are xored giving this way the output of the round function. The problem is to calculate the nonlinearity of such Boolean mapping when the component S-boxes are quite large, e.g. having 8-bit inputs and 32-bit outputs. In the CAST-like ciphers [1, 2] there was used the round function with four such S-boxes giving the mapping of 32-bit input and 32-bit output. The resistance of the CAST-like cipher to differential and linear cryptanalysis was investigated in [5]. At present, it is not possible in a direct way to calculate the nonlinearity of this round function. In the paper [11] the authors stated, without giving details, that they had calculated that nonlinearity and gave the numerical result. Following their suggestions we have proved here Lemma 4.3 and Theorem 4.4 which enable to calculate the nonlinearity of the function. The basic inspiration was taken from the notion of multi-dimensional Walsh transform as presented in [3], although its explicit definition is not presented here since we needed only its special case of separable variables. The examined round function is a good approximation of that one used in the cipher CAST-256 [2], where in two cases bitwise addition is replaced by algebraic operations like arithmetic addition and subtraction modulo 2^{32} . The estimation or the explicit calculation of the nonlinearity of round function is used to obtain the resistance of the cipher against linear cryptanalysis. The result is better when we consider the round function as a whole than that one obtained by taking into account the nonlinear properties of the individual S-boxes.

The paper is organized as follows. In section 2 we present the basic facts on Boolean functions, their nonlinearity and the fast Walsh transform. The section 3 describes the substitution boxes and their linear approximation tables. In section 4 there are investigated the nonlinear properties of the introduced round function. The Lemma 4.2 was given without proof in [11]. The Lemma 4.3 and Theorem 4.4 seem to be new ones. We have implemented the method and calculated the nonlinearity of the round function with four S-boxes taken from CAST-128 confirming the numerical value from [11]. In section 6 we give the application of our results to the linear cryptanalysis of the block cipher TGR which is a modification of the

hash function Tiger proposed by Anderson and Biham [4] working in the encryption mode. We have collected in the paper the proofs of facts on linear cryptanalysis and Walsh transform which are commonly known but in most cases are presented without proofs in the original papers.

2 Boolean Functions

A *Boolean function* with m inputs is a mapping $f : Z_2^m \rightarrow Z_2$, where $m \in \mathbf{N}$. The Boolean function $f : Z_2^m \rightarrow Z_2$ is an *affine* one when it can be represented as $f(\mathbf{x}) = a_m x_m \oplus a_{m-1} x_{m-1} \oplus \dots \oplus a_1 x_1 \oplus a_0$, where $\mathbf{x} = [x_m, x_{m-1}, \dots, x_1] \in Z_2^m$ and $a_i \in Z_2$, $i = 0, 1, \dots, m$. The affine function f is *linear* when $a_0 = 0$.

Let \mathbf{a}_i be n -dimensional binary vector being the binary representation of an integer i written in the decimal form, i.e. $\mathbf{a}_0 = [0, \dots, 0]$, $\mathbf{a}_1 = [0, \dots, 0, 1]$, \dots , $\mathbf{a}_{2^m-1} = [1, \dots, 1]$. Then the binary vector $[f(\mathbf{a}_0), f(\mathbf{a}_1), \dots, f(\mathbf{a}_{2^m-1})]$ is called the *truth table* of the Boolean function $f : Z_2^m \rightarrow Z_2$. The truth table uniquely describes the Boolean function, hence writing f we mean usually the binary vector representing its truth table.

For a given Boolean function f we define the *polar function* $\hat{f}(\mathbf{x}) = (-1)^{f(\mathbf{x})}$ which takes the values from the set $\{-1, 1\}$.

We denote $wt(\mathbf{a})$ the *Hamming weight* of the binary vector $\mathbf{a} = [a_m, a_{m-1}, \dots, a_1] \in Z_2^m$, which is the number of ones in \mathbf{a} , i.e. $wt(\mathbf{a}) = \sum_{i=1}^m a_i$. For given two vectors $\mathbf{a}, \mathbf{b} \in Z_2^m$ their

Hamming distance is defined as the number of places where the coordinates of these vectors are different, i.e. $d(\mathbf{a}, \mathbf{b}) = wt(\mathbf{a} \oplus \mathbf{b})$. For given two Boolean functions $f, g : Z_2^m \rightarrow Z_2$, their

Hamming distance is defined as the number of places at which are different their truth tables, i.e. $d(f, g) = \#\{\mathbf{x} \in Z_2^m \mid f(\mathbf{x}) \neq g(\mathbf{x})\} = wt(f \oplus g) = \sum_{\mathbf{x} \in Z_2^m} f(\mathbf{x}) \oplus g(\mathbf{x})$, where $wt(f \oplus g)$ is the

Hamming weight of the function $f \oplus g$.

Lemma 2.1

Let $f, g : Z_2^m \rightarrow Z_2$, then

$$d(f, g) = 2^{m-1} - \frac{1}{2} \sum_{\mathbf{x} \in Z_2^m} \hat{f}(\mathbf{x}) \hat{g}(\mathbf{x}).$$

Proof

Let $\hat{f} = [a_1, a_2, \dots, a_{2^m}]$, $\hat{g} = [b_1, b_2, \dots, b_{2^m}]$ and ρ_+ – the number of places where $a_i = b_i$,
 ρ_- – the number of places where $a_i \neq b_i$.

We can write

$$\sum_{\mathbf{x} \in Z_2^m} \hat{f}(\mathbf{x}) \hat{g}(\mathbf{x}) = \rho_+ - \rho_- = \rho_+ - \rho_- + (\rho_- - \rho_-) = \underbrace{\rho_+ + \rho_-}_{=2^m} - \rho_- - \rho_- = 2^m - 2\rho_-,$$

hence

$$\sum_{\mathbf{x} \in Z_2^m} \hat{f}(\mathbf{x}) \hat{g}(\mathbf{x}) = 2^m - 2\rho_-,$$

$$2\rho_- = 2^m - \sum_{\mathbf{x} \in Z_2^m} \hat{f}(\mathbf{x}) \hat{g}(\mathbf{x}),$$

$$\rho_- = 2^{m-1} - \frac{1}{2} \sum_{\mathbf{x} \in Z_2^m} \hat{f}(\mathbf{x}) \hat{g}(\mathbf{x}),$$

which is the thesis of the Lemma. ■

The real function of $\mathbf{u} \in Z_2^m$ defined as

$$W(f)(\mathbf{u}) = \sum_{\mathbf{x} \in Z_2^m} f(\mathbf{x}) \cdot (-1)^{\mathbf{u} \cdot \mathbf{x}}$$

is called the *Walsh transform* of the function f , where $f : Z_2^m \rightarrow \mathbf{R}$.

The Walsh transform of the polar function \hat{f} at the point \mathbf{u} is denoted $W(\hat{f})(\mathbf{u})$ or $\hat{W}(f)(\mathbf{u})$.

Lemma 2.2

For a Boolean function $f : Z_2^m \rightarrow Z_2$ and an affine function $A_{\mathbf{a},c}(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x} \oplus c$, where $\mathbf{a} \in Z_2^m, c \in Z_2$ we have

$$d(f, A_{\mathbf{a},c}) = \frac{1}{2} (2^m - (-1)^c W(\hat{f})(\mathbf{a})).$$

Proof

Using Lemma 2.1 one has

$$\begin{aligned} d(f, A_{\mathbf{a},c}) &= 2^{m-1} - \frac{1}{2} \sum_{\mathbf{x} \in Z_2^m} \hat{f}(\mathbf{x}) \hat{A}_{\mathbf{a},c}(\mathbf{x}) = 2^{m-1} - \frac{1}{2} \sum_{\mathbf{x} \in Z_2^m} \hat{f}(\mathbf{x}) (-1)^{A_{\mathbf{a},c}(\mathbf{x})} = \\ &= 2^{m-1} - \frac{1}{2} \sum_{\mathbf{x} \in Z_2^m} \hat{f}(\mathbf{x}) (-1)^{\mathbf{a} \cdot \mathbf{x} \oplus c} = 2^{m-1} - \frac{1}{2} \sum_{\mathbf{x} \in Z_2^m} \hat{f}(\mathbf{x}) (-1)^{\mathbf{a} \cdot \mathbf{x}} (-1)^c = \\ &= 2^{m-1} - \frac{1}{2} (-1)^c \sum_{\mathbf{x} \in Z_2^m} \hat{f}(\mathbf{x}) (-1)^{\mathbf{a} \cdot \mathbf{x}} = 2^{m-1} - \frac{1}{2} (-1)^c W(\hat{f})(\mathbf{a}) = \frac{1}{2} (2^m - (-1)^c W(\hat{f})(\mathbf{a})). \end{aligned}$$

■

Lemma 2.3

For a real constant c and a real function f defined on a finite domain D one has

$$\min_{x \in D} \{c - f(x), c + f(x)\} = c - \max_{x \in D} |f(x)|.$$

Proof

$$\begin{aligned} M &= \min_{x \in D} \{c - f(x), c + f(x)\} \Leftrightarrow \\ &\Leftrightarrow [\exists_{x \in D} c - f(x) = M \vee c + f(x) = M] \wedge [\forall_{x \in D} c - f(x) \geq M \wedge c + f(x) \geq M] \Leftrightarrow \\ &\Leftrightarrow [\exists_{x \in D} f(x) = c - M \vee -f(x) = c - M] \wedge [\forall_{x \in D} f(x) \leq c - M \wedge -f(x) \leq c - M] \Leftrightarrow \\ &\Leftrightarrow [\exists_{x \in D} |f(x)| = c - M] \wedge [\forall_{x \in D} |f(x)| \leq c - M] \Leftrightarrow \\ &\Leftrightarrow \max_{x \in D} |f(x)| = c - M \Leftrightarrow c - \max_{x \in D} |f(x)| = M. \end{aligned}$$

■

The *nonlinearity* of a Boolean function $f : Z_2^m \rightarrow Z_2$ is defined as

$$NL_f = \min_{\mathbf{a}, c} \# \{ \mathbf{x} \in Z_2^m \mid f(\mathbf{x}) \neq \mathbf{a} \cdot \mathbf{x} \oplus c \},$$

where $\mathbf{a} \in Z_2^m, c \in Z_2$. The nonlinearity of the Boolean function is its Hamming distance to the nearest affine function.

Lemma 2.4

Let $f : Z_2^m \rightarrow Z_2$, then

$$NL_f = 2^{m-1} - \frac{1}{2} \max_{\mathbf{a} \in Z_2^m} |W(\hat{f})(\mathbf{a})|.$$

Proof

$$NL_f = \min_{\substack{\mathbf{a} \in Z_2^m \\ c \in Z_2}} \# \{ \mathbf{x} \in Z_2^m \mid f(\mathbf{x}) \neq \mathbf{a} \cdot \mathbf{x} \oplus c \} = \min_{\substack{\mathbf{a} \in Z_2^m \\ c \in Z_2}} d(f, A_{\mathbf{a},c}) = \min_{\mathbf{a} \in Z_2^m} \{ d(f, A_{\mathbf{a},0}), d(f, A_{\mathbf{a},1}) \} = (*).$$

Using Lemma 2.2 one has

$$\begin{aligned} (*) &= \min_{\mathbf{a} \in Z_2^m} \left\{ \frac{1}{2} (2^m - (-1)^0 W(\hat{f})(\mathbf{a})), \frac{1}{2} (2^m - (-1)^1 W(\hat{f})(\mathbf{a})) \right\} = \\ &= \min_{\mathbf{a} \in Z_2^m} \left\{ 2^{m-1} - \frac{1}{2} W(\hat{f})(\mathbf{a}), 2^{m-1} + \frac{1}{2} W(\hat{f})(\mathbf{a}) \right\} = (**). \end{aligned}$$

and Lemma 2.3 gives

$$(**) = 2^{m-1} - \max_{\mathbf{a} \in Z_2^m} \left| \frac{1}{2} W(\hat{f})(\mathbf{a}) \right| = 2^{m-1} - \frac{1}{2} \max_{\mathbf{a} \in Z_2^m} |W(\hat{f})(\mathbf{a})|.$$

■

The effective method of calculating the nonlinearity of a Boolean function f must involve the fast calculating of the Walsh transform $W(\hat{f})$.

The *Walsh-Hadamard matrix* is defined as

$$H_m = \begin{bmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{bmatrix},$$

where $m = 1, 2, 3, \dots$ and $H_0 = 1$; which can be written as

$$H_m = H_1 \otimes H_{m-1},$$

where $H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and \otimes denotes the Kronecker product, e.g. for

$$A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}, \quad B = \begin{bmatrix} b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 \\ b_7 & b_8 & b_9 \end{bmatrix}$$

we have

$$A \otimes B = \begin{bmatrix} a_1 B & a_2 B \\ a_3 B & a_4 B \end{bmatrix}, \quad B \otimes A = \begin{bmatrix} b_1 A & b_2 A & b_3 A \\ b_4 A & b_5 A & b_6 A \\ b_7 A & b_8 A & b_9 A \end{bmatrix}.$$

One can observe that the Walsh-Hadamard matrix is a symmetric one: $H_m = H_m^T$.

Lemma 2.5

$$H_m = [(-1)^{\mathbf{u} \cdot \mathbf{v}}],$$

where $\mathbf{u}, \mathbf{v} \in Z_2^m$, $\mathbf{u} = [u_m, u_{m-1}, \dots, u_1]$, $\mathbf{v} = [v_m, v_{m-1}, \dots, v_1]$ and $\mathbf{u} = \alpha_i$, $\mathbf{v} = \alpha_j$, the indexes $i, j = 0, 1, \dots, 2^m - 1$ indicate the row and the column of the matrix H_m .

Proof (by induction)

$$\text{Let } m = 1, \text{ then } \mathbf{u}, \mathbf{v} \in Z_2 \text{ and } [(-1)^{\mathbf{u} \cdot \mathbf{v}}] = \begin{bmatrix} (-1)^{0 \cdot 0} & (-1)^{0 \cdot 1} \\ (-1)^{1 \cdot 0} & (-1)^{1 \cdot 1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H_1.$$

Let us assume the thesis of the Lemma is true for $m = 1, 2, \dots, k$. Then for $m = k + 1$ we have

$$H_{k+1} = H_1 \otimes H_k = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes [(-1)^{\mathbf{u} \cdot \mathbf{v}}],$$

where $\mathbf{u}, \mathbf{v} \in Z_2^k$, $\mathbf{u} = [u_k, u_{k-1}, \dots, u_1]$, $\mathbf{v} = [v_k, v_{k-1}, \dots, v_1]$.

We calculate

$$\begin{aligned} H_{k+1} &= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes [(-1)^{\mathbf{u} \cdot \mathbf{v}}] = \begin{bmatrix} (-1)^0 [(-1)^{\mathbf{u} \cdot \mathbf{v}}] & (-1)^0 [(-1)^{\mathbf{u} \cdot \mathbf{v}}] \\ (-1)^0 [(-1)^{\mathbf{u} \cdot \mathbf{v}}] & (-1)^1 [(-1)^{\mathbf{u} \cdot \mathbf{v}}] \end{bmatrix} = \\ &= \begin{bmatrix} (-1)^{u_{k+1} \cdot v_{k+1}} [(-1)^{\mathbf{u} \cdot \mathbf{v}}] & (-1)^{u_{k+1} \cdot v_{k+1}} [(-1)^{\mathbf{u} \cdot \mathbf{v}}] \\ (-1)^{u_{k+1} \cdot v_{k+1}} [(-1)^{\mathbf{u} \cdot \mathbf{v}}] & (-1)^{u_{k+1} \cdot v_{k+1}} [(-1)^{\mathbf{u} \cdot \mathbf{v}}] \end{bmatrix} = (*), \end{aligned}$$

where $u_{k+1}, v_{k+1} \in Z_2$ indicates the sub-matrices of the matrix H_{k+1} . Hence

(*) = $[(-1)^{\mathbf{u} \cdot \mathbf{v} \oplus u_{k+1} \cdot v_{k+1}}] = [(-1)^{\mathbf{u}' \cdot \mathbf{v}'}]$, where $\mathbf{u}', \mathbf{v}' \in Z_2^{k+1}$ and $\mathbf{u}' = [u_{k+1}, u_k, u_{k-1}, \dots, u_1]$, $\mathbf{v}' = [v_{k+1}, v_k, v_{k-1}, \dots, v_1]$. This implies that the thesis is true for arbitrary $m \geq 1$. ■

Lemma 2.6

The Walsh transform of the function $f : Z_2^m \rightarrow R$ can be represented as

$$W(f) = f \cdot H_m.$$

Proof

From the definition of the Walsh transform we have

$$W(f)(\mathbf{u}) = \sum_{\mathbf{x} \in Z_2^m} f(\mathbf{x}) \cdot (-1)^{\mathbf{u} \cdot \mathbf{x}} = f \cdot h_{\mathbf{u}}, \text{ where } h_{\mathbf{u}} = [(-1)^{\mathbf{u} \cdot \alpha_0}, (-1)^{\mathbf{u} \cdot \alpha_1}, \dots, (-1)^{\mathbf{u} \cdot \alpha_{2^m-1}}]^T.$$

Let us notice that $[h_{\mathbf{a}_0}, h_{\mathbf{a}_1}, \dots, h_{\mathbf{a}_{2^m-1}}]$ is the symmetric matrix $[(-1)^{\mathbf{a}_i \cdot \mathbf{a}_j}]$, where $i, j = 0, 1, \dots, 2^m-1$ are the row number and the column number of this matrix. Since $[h_{\mathbf{a}_0}, h_{\mathbf{a}_1}, \dots, h_{\mathbf{a}_{2^m-1}}] = [(-1)^{\mathbf{a}_i \cdot \mathbf{a}_j}]$, hence Lemma 2.5 gives $[h_{\mathbf{a}_0}, h_{\mathbf{a}_1}, \dots, h_{\mathbf{a}_{2^m-1}}] = H_m$, so $h_{\mathbf{a}_i}$ is the i -th column (and also the i -th row since the matrix is symmetric) of the Walsh-Hadamard matrix H_m . Hence the vector containing all values of the Walsh transform of the function f for the succeeding arguments $\mathbf{u} = \mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_{2^m-1}$ is equal to $W(f) = f \cdot [h_{\mathbf{a}_0}, h_{\mathbf{a}_1}, \dots, h_{\mathbf{a}_{2^m-1}}] = f \cdot H_m$.

■

Lemma 2.7

For arbitrary $x, y \in \mathbf{R}$ one has

$$\max\{|x+y|, |x-y|\} = |x| + |y|.$$

Proof

Let us notice that for x and y of the same sign it is $|x+y| \geq |x-y|$, in the opposite case

$|x+y| < |x-y|$. Let us consider the cases:

- 1) If $x, y \geq 0$, then $\max\{|x+y|, |x-y|\} = |x+y| = x+y = |x| + |y|$.
- 2) If $x, y < 0$, then $\max\{|x+y|, |x-y|\} = |x+y| = -(x+y) = (-x) + (-y) = |x| + |y|$.
- 3) If $x \geq 0, y < 0$, then $\max\{|x+y|, |x-y|\} = |x-y| = x-y = x + (-y) = |x| + |y|$.
- 4) If $x < 0, y \geq 0$, then $\max\{|x+y|, |x-y|\} = |x-y| = -(x-y) = (-x) + y = |x| + |y|$.

■

Let $f : Z_2^m \rightarrow Z_2$ be a Boolean function and \hat{f} its polar form. Let $\hat{f}_{[i \dots j]}$ represents the truth table of \hat{f} for the inputs from \mathbf{a}_i to \mathbf{a}_j . Then the Lemma 2.6 gives

$$W(\hat{f}) = \hat{f} \cdot H_m = \hat{f}_{[0 \dots 2^m-1]} \cdot H_m = [\hat{f}_{[0 \dots 2^{m-1}-1]}, \hat{f}_{[2^{m-1} \dots 2^m-1]}] \cdot \begin{bmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{bmatrix} = [W_0 + W_1, W_0 - W_1],$$

where $W_0 = \hat{f}_{[0 \dots 2^{m-1}-1]} \cdot H_{m-1}$ and $W_1 = \hat{f}_{[2^{m-1} \dots 2^m-1]} \cdot H_{m-1}$. This way to calculate the Walsh transform of the function $\hat{f} : Z_2^m \rightarrow \{-1, 1\}$ it is sufficient to know the transforms W_0, W_1 of the functions $\hat{f}_0, \hat{f}_1 : Z_2^{m-1} \rightarrow \{-1, 1\}$, where $\hat{f} = [\hat{f}_0, \hat{f}_1]$.

To speed up the calculation of the Walsh transform one can create in the computer memory the matrix $W4$ having dimension $p \times q$, where $p = 2^{2^4} = 65536$, $q = 2^4 = 16$, which has rows indexed by the successive 16-bit vectors f_i^4 , $i = 0, \dots, 65535$ (being the truth tables of Boolean functions of 4 variables) and the columns are indexed by the successive 4-bit vectors α_j ($j = 0, \dots, 15$). The (i, j) -entry of the matrix $W4$ is the value of Walsh transform $W(\hat{f}_i^4)(\alpha_j)$. To calculate the Walsh transform of the function $\hat{f}^5 : Z_2^5 \rightarrow \{-1, 1\}$, its truth table is divided into two halves which are the truth tables of the functions $\hat{f}_i^4, \hat{f}_j^4 : Z_2^4 \rightarrow \{-1, 1\}$. Then we calculate $W(\hat{f}^5)(k) = W4(i, k) + W4(j, k)$ and $W(\hat{f}^5)(k + 16) = W4(i, k) - W4(j, k)$, where $k = 0, \dots, 15$. We follow in a similar way for function having more inputs, e.g. to calculate $W(\hat{f}^6)$ we divide the truth table of function having 6 inputs into two truth tables of functions having 5 inputs and in turn into four truth tables of 4-input functions.

If we calculate $W(\hat{f}) = [W_0 + W_1, W_0 - W_1]$ to obtain the nonlinearity of f , then from Lemma 2.4 we need $\max_{\mathbf{u} \in Z_2^m} |W(\hat{f})(\mathbf{u})|$ and from Lemma 2.7 we can in the last step of calculation of Walsh transform limit to take the maximum over the elements of $|W_0| + |W_1|$.

3 Substitution Boxes

A *substitution box* of dimension $m \times n$ is a transformation $S : Z_2^m \rightarrow Z_2^n$, where $m, n \in \mathbf{N}$. The substitution box S can be considered as a collection of its coordinates n Boolean functions, i.e. $S = [f_n, f_{n-1}, \dots, f_1]$, where $f_i : Z_2^m \rightarrow Z_2$.

The *nonlinearity* of substitution box $S : Z_2^m \rightarrow Z_2^n$ is defined as

$$NL_S = \min_{\mathbf{b}} NL_{\mathbf{b}, S},$$

where $\mathbf{b} \in Z_2^n \setminus \{\mathbf{0}\}$, $\mathbf{b} = [b_n, b_{n-1}, \dots, b_1]$ and $NL_{\mathbf{b}, S}$ is nonlinearity of the Boolean function $\mathbf{b} \cdot S = b_n f_n \oplus b_{n-1} f_{n-1} \oplus \dots \oplus b_1 f_1$.

For a given substitution box $S : Z_2^m \rightarrow Z_2^n$ it is defined the *linear approximation table* which elements are

$$LAT_S(\mathbf{a}, \mathbf{b}) = \#\{\mathbf{x} \in Z_2^m \mid \mathbf{a} \cdot \mathbf{x} = \mathbf{b} \cdot S(\mathbf{x})\} - 2^{m-1},$$

where $\mathbf{a} \in Z_2^m, \mathbf{b} \in Z_2^n \setminus \{\mathbf{0}\}$.

Lemma 3.1

For a substitution box $S : Z_2^m \rightarrow Z_2^n$ we have

$$LAT_S(\mathbf{a}, \mathbf{b}) = 2^{m-1} - d(\mathbf{a} \cdot \mathbf{x}, \mathbf{b} \cdot S),$$

where $\mathbf{a} \in Z_2^m, \mathbf{b} \in Z_2^n \setminus \{\mathbf{0}\}$.

Proof

$$\begin{aligned} LAT_S(\mathbf{a}, \mathbf{b}) &= \#\{\mathbf{x} \in Z_2^m \mid \mathbf{a} \cdot \mathbf{x} = \mathbf{b} \cdot S(\mathbf{x})\} - 2^{m-1} = 2^m - \#\{\mathbf{x} \in Z_2^m \mid \mathbf{a} \cdot \mathbf{x} \neq \mathbf{b} \cdot S(\mathbf{x})\} - 2^{m-1} = \\ &= 2^{m-1} - d(\mathbf{a} \cdot \mathbf{x}, \mathbf{b} \cdot S). \end{aligned}$$

■

Lemma 3.2

For a substitution box $S : Z_2^m \rightarrow Z_2^n$ one has

$$NL_S = 2^{m-1} - \max_{\mathbf{a}, \mathbf{b}} |LAT_S(\mathbf{a}, \mathbf{b})|,$$

where $\mathbf{a} \in Z_2^m, \mathbf{b} \in Z_2^n \setminus \{\mathbf{0}\}$.

Proof

$$\begin{aligned} NL_S &= \min_{\mathbf{b}} NL_{\mathbf{b}, S} = \min_{\mathbf{a}, \mathbf{b}, c} \#\{\mathbf{x} \in Z_2^m \mid \mathbf{b} \cdot S(\mathbf{x}) \neq \mathbf{a} \cdot \mathbf{x} \oplus c\} = \\ &= \min_{\mathbf{a}, \mathbf{b}} \#\{\mathbf{x} \in Z_2^m \mid \mathbf{b} \cdot S(\mathbf{x}) \neq \mathbf{a} \cdot \mathbf{x} \vee \mathbf{b} \cdot S(\mathbf{x}) \neq \mathbf{a} \cdot \mathbf{x} \oplus 1\} = \\ &= \min_{\mathbf{a}, \mathbf{b}} \{d(\mathbf{b} \cdot S, \mathbf{a} \cdot \mathbf{x}), d(\mathbf{b} \cdot S, \mathbf{a} \cdot \mathbf{x} \oplus 1)\} = \min_{\mathbf{a}, \mathbf{b}} \{d(\mathbf{b} \cdot S, \mathbf{a} \cdot \mathbf{x}), 2^m - d(\mathbf{b} \cdot S, \mathbf{a} \cdot \mathbf{x})\} = \\ &= 2^{m-1} + \min_{\mathbf{a}, \mathbf{b}} \{d(\mathbf{b} \cdot S, \mathbf{a} \cdot \mathbf{x}) - 2^{m-1}, 2^{m-1} - d(\mathbf{b} \cdot S, \mathbf{a} \cdot \mathbf{x})\} = (*) \end{aligned}$$

From Lemma 3.1 and next from Lemma 2.3 we obtain

$$(*) = 2^{m-1} + \min_{\mathbf{a}, \mathbf{b}} \{-LAT_S(\mathbf{a}, \mathbf{b}), LAT_S(\mathbf{a}, \mathbf{b})\} = 2^{m-1} - \max_{\mathbf{a}, \mathbf{b}} |LAT_S(\mathbf{a}, \mathbf{b})| .$$

■

By the *linear approximation* of a substitution box $S : Z_2^m \rightarrow Z_2^n$ we mean the equation

$$\mathbf{a} \cdot \mathbf{x} = \mathbf{b} \cdot S(\mathbf{x}),$$

where $\mathbf{a} \in Z_2^m, \mathbf{b} \in Z_2^n \setminus \{\mathbf{0}\}$. Let p be the probability of satisfying this equation for given \mathbf{a} and

\mathbf{b} , it is

$$p = \frac{\#\{\mathbf{x} \in Z_2^m \mid \mathbf{a} \cdot \mathbf{x} = \mathbf{b} \cdot S(\mathbf{x})\}}{2^m}.$$

Then

$$\left| p - \frac{1}{2} \right| = \left| \frac{\#\{\mathbf{x} \in Z_2^m \mid \mathbf{a} \cdot \mathbf{x} = \mathbf{b} \cdot S(\mathbf{x})\} - 2^{m-1}}{2^m} \right| = \frac{|LAT(\mathbf{a}, \mathbf{b})|}{2^m}$$

has a meaning of efficiency of the linear approximation of substitution box $S : Z_2^m \rightarrow Z_2^n$.

Let p_β denotes the probability of best linear approximation, it means that one for which the

efficiency $\left| p_\beta - \frac{1}{2} \right|$ has the biggest value.

Lemma 3.3 (Lee et al. [5])

For a substitution box $S : Z_2^m \rightarrow Z_2^n$ it is

$$\left| p_\beta - \frac{1}{2} \right| = \frac{2^{m-1} - NL_S}{2^m}.$$

Proof

By definition $\left| p_\beta - \frac{1}{2} \right| = \frac{\max_{\mathbf{a}, \mathbf{b}} |LAT(\mathbf{a}, \mathbf{b})|}{2^m}$ and by the Lemma 3.2 we have

$$NL_S = 2^{m-1} - \max_{\mathbf{a}, \mathbf{b}} |LAT_S(\mathbf{a}, \mathbf{b})|, \text{ hence } \max_{\mathbf{a}, \mathbf{b}} |LAT_S(\mathbf{a}, \mathbf{b})| = 2^{m-1} - NL_S \text{ and } \left| p_\beta - \frac{1}{2} \right| =$$

$$= \frac{\max_{\mathbf{a}, \mathbf{b}} |LAT(\mathbf{a}, \mathbf{b})|}{2^m} = \frac{2^{m-1} - NL_S}{2^m}.$$

■

4 The Nonlinearity of the Round Function

Let $F : Z_2^{km} \rightarrow Z_2^n$ be a transformation such that

$$F(\mathbf{x}) = F(\mathbf{x}_k, \mathbf{x}_{k-1}, \dots, \mathbf{x}_1) = S_1(\mathbf{x}_1) \oplus S_2(\mathbf{x}_2) \oplus \dots \oplus S_k(\mathbf{x}_k),$$

where $S_i : Z_2^m \rightarrow Z_2^n, i = 1, 2, \dots, k$ and $S_i = [f_{i,n}, f_{i,n-1}, \dots, f_{i,1}]$, $f_{i,j} : Z_2^m \rightarrow Z_2, j = 1, 2, \dots, n$.

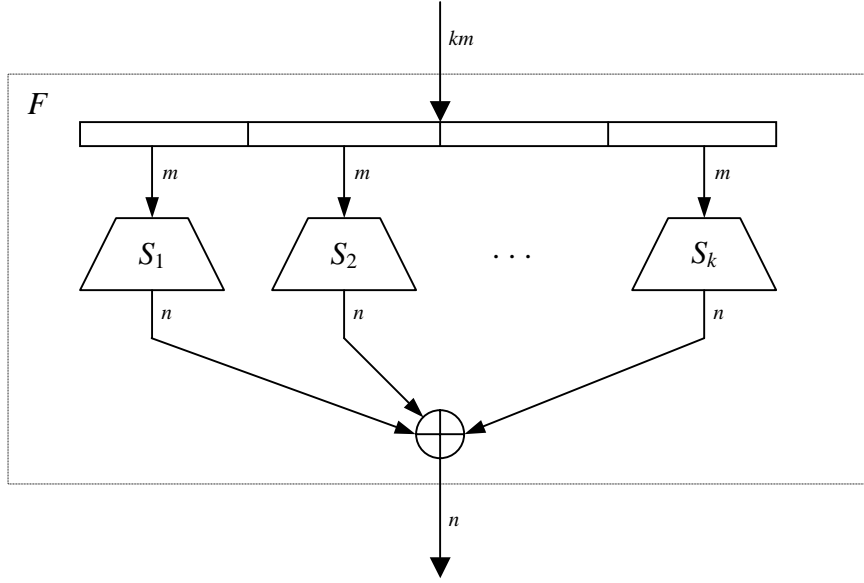


Figure 4.1: The structure of F round function.

Similarly to substitution boxes it is defined the nonlinearity of the transformation

$$F : Z_2^{km} \rightarrow Z_2^n :$$

$$NL_F = \min_{\mathbf{b}} NL_{\mathbf{b},F}, \quad (4.1)$$

where $\mathbf{b} \in Z_2^n \setminus \{\mathbf{0}\}$, $\mathbf{b} = [b_n, b_{n-1}, \dots, b_1]$, $F = [F_n, F_{n-1}, \dots, F_1]$, $F_j : Z_2^{km} \rightarrow Z_2$,

$F_j(\mathbf{x}) = F_j(\mathbf{x}_k, \mathbf{x}_{k-1}, \dots, \mathbf{x}_1) = f_{1,j}(\mathbf{x}_1) \oplus f_{2,j}(\mathbf{x}_2) \oplus \dots \oplus f_{k,j}(\mathbf{x}_k)$ and $NL_{\mathbf{b},F}$ is nonlinearity of the Boolean function $\mathbf{b} \cdot F = b_n F_n \oplus b_{n-1} F_{n-1} \oplus \dots \oplus b_1 F_1$.

Lemma 4.1 (Piling-Up Lemma, Matsui [6])

Let X_1, X_2, \dots, X_n be independent binary random variables, where $n \geq 2$ and let $P\{X_i = 0\} = p_i$, $P\{X_i = 1\} = 1 - p_i$ for $i = 1, 2, \dots, n$. Then

$$P\{X_1 \oplus X_2 \oplus \dots \oplus X_n = 0\} = \frac{1}{2} + 2^{n-1} \prod_{i=1}^n (p_i - \frac{1}{2}) = \frac{1}{2} + 2^{n-1} \prod_{i=1}^n \varepsilon_i,$$

where $p_i = \frac{1}{2} + \varepsilon_i$, $-\frac{1}{2} \leq \varepsilon_i \leq \frac{1}{2}$.

Proof (by induction)

Let $n = 2$, then

$$\begin{aligned} P\{X_1 \oplus X_2 = 0\} &= P\{X_1 = X_2\} = P\{X_1 = 0, X_2 = 0\} + P\{X_1 = 1, X_2 = 1\} = \\ &= p_1 p_2 + (1 - p_1)(1 - p_2) = (\frac{1}{2} + \varepsilon_1)(\frac{1}{2} + \varepsilon_2) + (\frac{1}{2} - \varepsilon_1)(\frac{1}{2} - \varepsilon_2) = \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{4} + \frac{1}{2}\varepsilon_2 + \frac{1}{2}\varepsilon_1 + \varepsilon_1\varepsilon_2 + \frac{1}{4} - \frac{1}{2}\varepsilon_2 - \frac{1}{2}\varepsilon_1 + \varepsilon_1\varepsilon_2 = \\
&= \frac{1}{2} + 2\varepsilon_1\varepsilon_2 = \frac{1}{2} + 2(p_1 - \frac{1}{2})(p_2 - \frac{1}{2}).
\end{aligned}$$

Let us assume the thesis of the Lemma is true for $n = 2, 3, \dots, k$. Then for $n = k + 1$ we have

$$\begin{aligned}
&\mathbb{P}\{X_1 \oplus X_2 \oplus \dots \oplus X_k \oplus X_{k+1} = 0\} = \\
&= \mathbb{P}\{X_1 \oplus X_2 \oplus \dots \oplus X_k = 0, X_{k+1} = 0\} + \mathbb{P}\{X_1 \oplus X_2 \oplus \dots \oplus X_k = 1, X_{k+1} = 1\} = \\
&= \left(\frac{1}{2} + 2^{k-1} \prod_{i=1}^k (p_i - \frac{1}{2}) \right) p_{k+1} + \left(1 - \frac{1}{2} - 2^{k-1} \prod_{i=1}^k (p_i - \frac{1}{2}) \right) (1 - p_{k+1}) = \\
&= \left(\frac{1}{2} + 2^{k-1} \prod_{i=1}^k \varepsilon_i \right) \left(\frac{1}{2} + \varepsilon_{k+1} \right) + \left(\frac{1}{2} - 2^{k-1} \prod_{i=1}^k \varepsilon_i \right) \left(\frac{1}{2} - \varepsilon_{k+1} \right) = \\
&= \frac{1}{4} + \frac{1}{2}\varepsilon_{k+1} + 2^{k-2} \prod_{i=1}^k \varepsilon_i + 2^{k-1} \prod_{i=1}^{k+1} \varepsilon_i + \frac{1}{4} - \frac{1}{2}\varepsilon_{k+1} - 2^{k-2} \prod_{i=1}^k \varepsilon_i + 2^{k-1} \prod_{i=1}^{k+1} \varepsilon_i = \\
&= \frac{1}{2} + 2^k \prod_{i=1}^{k+1} \varepsilon_i = \frac{1}{2} + 2^k \prod_{i=1}^{k+1} (p_i - \frac{1}{2}).
\end{aligned}$$

The calculation above implies that the thesis is true for $n \geq 2$. ■

The following lemma is a generalization of the result given without proof by Youssef, Chen and Tavares in [11].

Lemma 4.2

$$NL_F \geq 2^{km-1} - 2^{k-1} \prod_{i=1}^k (2^{m-1} - NL_{S_i}).$$

Proof

Let us take the linear approximation of the transformation F :

$$\mathbf{a} \cdot \mathbf{x} = \mathbf{b} \cdot F(\mathbf{x}),$$

where $\mathbf{a} \in \mathbb{Z}_2^{km}$, $\mathbf{b} \in \mathbb{Z}_2^n \setminus \{\mathbf{0}\}$, in other words

$$\mathbf{a}_1 \mathbf{x}_1 \oplus \mathbf{a}_2 \mathbf{x}_2 \oplus \dots \oplus \mathbf{a}_k \mathbf{x}_k = \mathbf{b}_1 S_1(\mathbf{x}_1) \oplus \mathbf{b}_2 S_2(\mathbf{x}_2) \oplus \dots \oplus \mathbf{b}_k S_k(\mathbf{x}_k).$$

Let p_β denotes the probability of the linear approximation of transformation F having the best

efficiency, then by Lemma 3.3 we have $\left| p_\beta - \frac{1}{2} \right| = \frac{2^{km-1} - NL_F}{2^{km}}$.

Let us consider generalization of the above approximation, it is

$$\mathbf{a}_1 \mathbf{x}_1 \oplus \mathbf{a}_2 \mathbf{x}_2 \oplus \dots \oplus \mathbf{a}_k \mathbf{x}_k = \mathbf{b}_1 S_1(\mathbf{x}_1) \oplus \mathbf{b}_2 S_2(\mathbf{x}_2) \oplus \dots \oplus \mathbf{b}_k S_k(\mathbf{x}_k),$$

where $\mathbf{a}_i \in \mathbb{Z}_2^m, \mathbf{b}_i \in \mathbb{Z}_2^n \setminus \{\mathbf{0}\}$. Let p_γ denotes the probability of generalized approximation having the best efficiency. Then $\left|p_\beta - \frac{1}{2}\right| \leq \left|p_\gamma - \frac{1}{2}\right|$, since in the worst case we can take $\mathbf{b}_1 = \mathbf{b}_2 = \dots = \mathbf{b}_k = \mathbf{b}$. Let us transform the generalized approximation to the form

$$\mathbf{a}_1 \mathbf{x}_1 \oplus \mathbf{b}_1 S_1(\mathbf{x}_1) \oplus \mathbf{a}_2 \mathbf{x}_2 \oplus \mathbf{b}_2 S_2(\mathbf{x}_2) \oplus \dots \oplus \mathbf{a}_k \mathbf{x}_k \oplus \mathbf{b}_k S_k(\mathbf{x}_k) = 0.$$

We assume that $X_i = \mathbf{a}_i \mathbf{x}_i \oplus \mathbf{b}_i S_i(\mathbf{x}_i)$ are independent binary random variables having the probability distribution $P\{X_i = 0\} = p_i, P\{X_i = 1\} = 1 - p_i$. This assumption is very natural since p_i are the probabilities of linear approximation of independent substitutions boxes S_i . By Lemma 4.1 we have

$$p = P\{X_1 \oplus X_2 \oplus \dots \oplus X_k = 0\} = \frac{1}{2} + 2^{k-1} \prod_{i=1}^k (p_i - \frac{1}{2}),$$

$$\left|p - \frac{1}{2}\right| = 2^{k-1} \prod_{i=1}^k \left|p_i - \frac{1}{2}\right|.$$

If we take the approximations of substitutions boxes having the best efficiency, which probabilities are equal $p_{\beta_1}, p_{\beta_2}, \dots, p_{\beta_k}$ respectively, then

$$2^{k-1} \prod_{i=1}^k \left|p_{\beta_i} - \frac{1}{2}\right| = \left|p_\gamma - \frac{1}{2}\right|.$$

Since $\left|p_\beta - \frac{1}{2}\right| \leq \left|p_\gamma - \frac{1}{2}\right|$, hence $\frac{2^{km-1} - NL_F}{2^{km}} \leq 2^{k-1} \prod_{i=1}^k \left|p_{\beta_i} - \frac{1}{2}\right|$

and consequently

$$NL_F \geq 2^{km-1} - 2^{k(m+1)-1} \prod_{i=1}^k \left|p_{\beta_i} - \frac{1}{2}\right|.$$

By Lemma 3.3 we obtain

$$\begin{aligned} NL_F &\geq 2^{km-1} - 2^{k(m+1)-1} \prod_{i=1}^k \left|p_{\beta_i} - \frac{1}{2}\right| = 2^{km-1} - 2^{k(m+1)-1} \prod_{i=1}^k \left(\frac{2^{m-1} - NL_{S_i}}{2^m}\right) = \\ &= 2^{km-1} - 2^{k(m+1)-1} \prod_{i=1}^k \left(\frac{2^m - 2NL_{S_i}}{2^{m+1}}\right) = 2^{km-1} - 2^{k(m+1)-1-k(m+1)} \prod_{i=1}^k (2^m - 2NL_{S_i}) = \\ &= 2^{km-1} - \frac{1}{2} \prod_{i=1}^k (2^m - 2NL_{S_i}) = 2^{km-1} - 2^{k-1} \prod_{i=1}^k (2^{m-1} - NL_{S_i}). \end{aligned}$$

■

Lemma 4.3

$$\widehat{W}(\mathbf{b} \cdot F)(\mathbf{u}) = \widehat{W}(\mathbf{b} \cdot S_1)(\mathbf{u}_1) \widehat{W}(\mathbf{b} \cdot S_2)(\mathbf{u}_2) \dots \widehat{W}(\mathbf{b} \cdot S_k)(\mathbf{u}_k),$$

where $\mathbf{u} = [\mathbf{u}_k, \mathbf{u}_{k-1}, \dots, \mathbf{u}_1]$.

Proof

Since $\mathbf{b} \cdot F = b_n F_n \oplus b_{n-1} F_{n-1} \oplus \dots \oplus b_1 F_1$ for $F = [F_n, F_{n-1}, \dots, F_1]$, $F_j : Z_2^{km} \rightarrow Z_2$,

$$F_j(\mathbf{x}) = F_j(\mathbf{x}_k, \mathbf{x}_{k-1}, \dots, \mathbf{x}_1) = f_{1,j}(\mathbf{x}_1) \oplus f_{2,j}(\mathbf{x}_2) \oplus \dots \oplus f_{k,j}(\mathbf{x}_k),$$

we have

$$\begin{aligned} \mathbf{b} \cdot F(\mathbf{x}) &= b_n F_n(\mathbf{x}) \oplus b_{n-1} F_{n-1}(\mathbf{x}) \oplus \dots \oplus b_1 F_1(\mathbf{x}) = \\ &= b_n (f_{1,n}(\mathbf{x}_1) \oplus f_{2,n}(\mathbf{x}_2) \oplus \dots \oplus f_{k,n}(\mathbf{x}_k)) \oplus b_{n-1} (f_{1,n-1}(\mathbf{x}_1) \oplus f_{2,n-1}(\mathbf{x}_2) \oplus \dots \oplus f_{k,n-1}(\mathbf{x}_k)) \oplus \dots \oplus \\ &= b_1 (f_{1,1}(\mathbf{x}_1) \oplus f_{2,1}(\mathbf{x}_2) \oplus \dots \oplus f_{k,1}(\mathbf{x}_k)) = \\ &= b_n f_{1,n}(\mathbf{x}_1) \oplus b_{n-1} f_{1,n-1}(\mathbf{x}_1) \oplus \dots \oplus b_1 f_{1,1}(\mathbf{x}_1) \oplus \\ &\oplus b_n f_{2,n}(\mathbf{x}_2) \oplus b_{n-1} f_{2,n-1}(\mathbf{x}_2) \oplus \dots \oplus b_1 f_{2,1}(\mathbf{x}_2) \oplus \dots \oplus \\ &\oplus b_n f_{k,n}(\mathbf{x}_k) \oplus b_{n-1} f_{k,n-1}(\mathbf{x}_k) \oplus \dots \oplus b_1 f_{k,1}(\mathbf{x}_k) = \mathbf{b} \cdot S_1(\mathbf{x}_1) \oplus \mathbf{b} \cdot S_2(\mathbf{x}_2) \oplus \dots \oplus \mathbf{b} \cdot S_k(\mathbf{x}_k). \end{aligned}$$

Then

$$\begin{aligned} \widehat{W}(\mathbf{b} \cdot F)(\mathbf{u}) &= \sum_{\mathbf{x} \in Z_2^{km}} (-1)^{\mathbf{b} \cdot F(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}} = \sum_{\substack{\mathbf{x}=[\mathbf{x}_k, \mathbf{x}_{k-1}, \dots, \mathbf{x}_1] \\ \mathbf{x}_j \in Z_2^m}} (-1)^{\mathbf{b} \cdot (S_1(\mathbf{x}_1) \oplus S_2(\mathbf{x}_2) \oplus \dots \oplus S_k(\mathbf{x}_k))} (-1)^{[\mathbf{u}_k, \mathbf{u}_{k-1}, \dots, \mathbf{u}_1] \cdot [\mathbf{x}_k, \mathbf{x}_{k-1}, \dots, \mathbf{x}_1]} = \\ &= \sum_{\mathbf{x}_k \in Z_2^m} \sum_{\mathbf{x}_{k-1} \in Z_2^m} \dots \sum_{\mathbf{x}_1 \in Z_2^m} (-1)^{\mathbf{b} \cdot S_1(\mathbf{x}_1) \oplus \mathbf{b} \cdot S_2(\mathbf{x}_2) \oplus \dots \oplus \mathbf{b} \cdot S_k(\mathbf{x}_k)} (-1)^{\mathbf{u}_1 \cdot \mathbf{x}_1 \oplus \mathbf{u}_2 \cdot \mathbf{x}_2 \oplus \dots \oplus \mathbf{u}_k \cdot \mathbf{x}_k} = \\ &= \sum_{\mathbf{x}_1 \in Z_2^m} (-1)^{\mathbf{b} \cdot S_1(\mathbf{x}_1)} (-1)^{\mathbf{u}_1 \cdot \mathbf{x}_1} \sum_{\mathbf{x}_2 \in Z_2^m} (-1)^{\mathbf{b} \cdot S_2(\mathbf{x}_2)} (-1)^{\mathbf{u}_2 \cdot \mathbf{x}_2} \dots \sum_{\mathbf{x}_k \in Z_2^m} (-1)^{\mathbf{b} \cdot S_k(\mathbf{x}_k)} (-1)^{\mathbf{u}_k \cdot \mathbf{x}_k} = \\ &= \widehat{W}(\mathbf{b} \cdot S_1)(\mathbf{u}_1) \widehat{W}(\mathbf{b} \cdot S_2)(\mathbf{u}_2) \dots \widehat{W}(\mathbf{b} \cdot S_k)(\mathbf{u}_k). \end{aligned}$$

■

Theorem 4.4

$$NL_{\mathbf{b} \cdot F} = 2^{km-1} - 2^{k-1} \prod_{i=1}^k (2^{m-1} - NL_{\mathbf{b} \cdot S_i}).$$

Proof

By Lemma 2.4 $NL_{\mathbf{b} \cdot F} = 2^{km-1} - \frac{1}{2} \max_{\mathbf{u} \in Z_2^{km}} |\widehat{W}(\mathbf{b} \cdot F)(\mathbf{u})|$ and by Lemma 4.3

$$\widehat{W}(\mathbf{b} \cdot F)(\mathbf{u}) = \widehat{W}(\mathbf{b} \cdot S_1)(\mathbf{u}_1) \widehat{W}(\mathbf{b} \cdot S_2)(\mathbf{u}_2) \dots \widehat{W}(\mathbf{b} \cdot S_k)(\mathbf{u}_k),$$

hence

$$\begin{aligned}
NL_{\mathbf{b},F} &= 2^{km-1} - \frac{1}{2} \max_{\substack{\mathbf{u} \in Z_2^{km} \\ \mathbf{u}=(\mathbf{u}_k, \mathbf{u}_{k-1}, \dots, \mathbf{u}_1)}} \left| \widehat{W}(\mathbf{b} \cdot S_1)(\mathbf{u}_1) \widehat{W}(\mathbf{b} \cdot S_2)(\mathbf{u}_2) \dots \widehat{W}(\mathbf{b} \cdot S_k)(\mathbf{u}_k) \right| = \\
&= 2^{km-1} - \frac{1}{2} \max_{\mathbf{u}_1 \in Z_2^m} \left| \widehat{W}(\mathbf{b} \cdot S_1)(\mathbf{u}_1) \right| \max_{\mathbf{u}_2 \in Z_2^m} \left| \widehat{W}(\mathbf{b} \cdot S_2)(\mathbf{u}_2) \right| \dots \max_{\mathbf{u}_k \in Z_2^m} \left| \widehat{W}(\mathbf{b} \cdot S_k)(\mathbf{u}_k) \right|.
\end{aligned}$$

Since $NL_{\mathbf{b},S_i} = 2^{m-1} - \frac{1}{2} \max_{\mathbf{u} \in Z_2^m} \left| \widehat{W}(\mathbf{b} \cdot S_i)(\mathbf{u}) \right|$, it means $\max_{\mathbf{u} \in Z_2^m} \left| \widehat{W}(\mathbf{b} \cdot S_i)(\mathbf{u}) \right| = 2^m - 2NL_{\mathbf{b},S_i}$,

and consequently

$$NL_{\mathbf{b},F} = 2^{km-1} - \frac{1}{2} \prod_{i=1}^k (2^m - 2NL_{\mathbf{b},S_i}) = 2^{km-1} - 2^{k-1} \prod_{i=1}^k (2^{m-1} - NL_{\mathbf{b},S_i}).$$

■

The above theorem has been used to calculate in the special cases the nonlinearity of the function F according to the formula (4.1).

5 The TGR Algorithm

The TGR algorithm is a block cipher which works on 128-bit blocks and uses 256-bit keys. The general scheme of the cipher TGR is shown in the Figure 5.1. The 128-bit plaintext P is transformed to the 128-bit ciphertext C in three passes ($r = 1, 2, 3$) each consisting of eight rounds ($j = 0, 1, \dots, 7$).

The passes use the 256-bit keys K_r obtained from the main 256-bit key K using the key schedule algorithm Key_sch . We have $K_r = Key_sch(K_{r-1})$, where $K_0 = K$. Each key K_r is divided into eight 32-bit subkeys $k_{r,j}$, which are used in the corresponding j -th round of the r -th pass. The first use of Key_sch has as an input the main key $K = (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7)$ and gives as an output the key $K_1 = (k_{1,0}, k_{1,1}, k_{1,2}, k_{1,3}, k_{1,4}, k_{1,5}, k_{1,6}, k_{1,7})$ used in the first pass. Next we have as an input to Key_sch the key K_1 and we get as an output $K_2 = (k_{2,0}, k_{2,1}, k_{2,2}, k_{2,3}, k_{2,4}, k_{2,5}, k_{2,6}, k_{2,7})$ and analogously for $K_3 = (k_{3,0}, k_{3,1}, k_{3,2}, k_{3,3}, k_{3,4}, k_{3,5}, k_{3,6}, k_{3,7})$. The Key_sch is described by the formulae shown in Figure 5.2. Operations like $+$ and $-$ are just an addition and a subtraction modulo 2^{32} respectively, \oplus is a bitwise sum modulo 2, \sim denotes a bitwise negation, \ll and \gg are bitwise shifts left and right respectively (the loosing bits are complemented by zeros), \lll and \ggg are bitwise rotations left and right respectively.

The 128-bit input to the j -th round of the r -th pass is divided into four 32-bit blocks denoted $(A_{r,j}, B_{r,j}, C_{r,j}, D_{r,j})$ and the 128-bit output of this round is denoted $(A'_{r,j}, B'_{r,j}, C'_{r,j}, D'_{r,j})$.

$D'_{r,j}$). The structure of the round is depicted in the Figure 5.3. The S-boxes S_1, S_2, S_3, S_4 are taken from the CAST-256 cipher [2] and operation Rot is the data-dependent rotation function just taken from the RC6 cipher [10] as shown in Figure 5.4.

The TGR design is based on the hash function Tiger proposed by Anderson and Biham in [4].

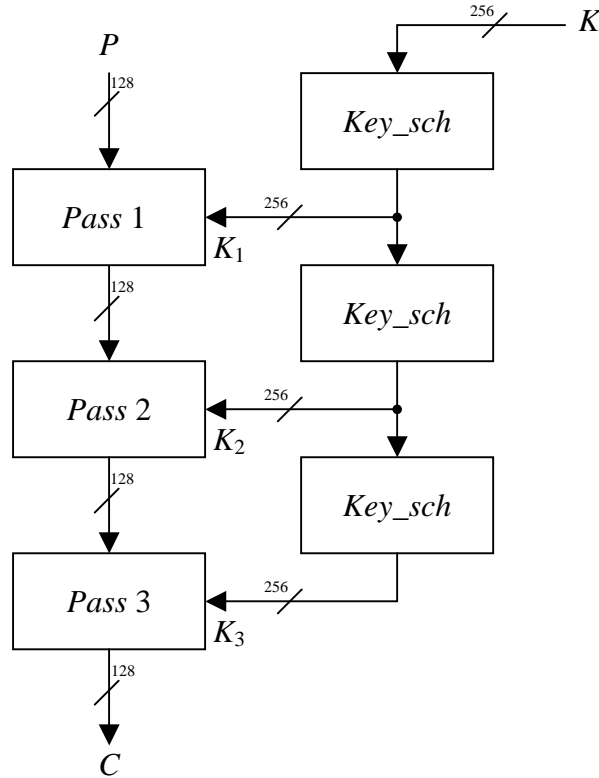


Figure 5.1. The scheme of the TGR encryption algorithm.

$$\begin{aligned}
 k_0 &:= k_0 - (k_7 \oplus ((\sim k_6) \lll 11) \oplus 0xa5a5a5a5) \\
 k_1 &:= k_1 \oplus k_0 \\
 k_2 &:= k_2 + k_1 \\
 k_3 &:= k_3 - (k_2 \oplus ((\sim k_1) \ggg 13)) \\
 k_4 &:= k_4 \oplus k_3 \\
 k_5 &:= k_5 + k_4 \\
 k_6 &:= k_6 - (k_5 \oplus ((\sim k_4) \gg 7)) \\
 k_7 &:= k_7 \oplus k_6 \\
 k_0 &:= k_0 + k_7 \\
 k_1 &:= k_1 - (k_0 \oplus ((\sim k_7) \ll 5)) \\
 k_2 &:= k_2 \oplus k_1 \\
 k_3 &:= k_3 + k_2
 \end{aligned}$$

$$\begin{aligned}
k_4 &:= k_4 - (k_3 \oplus ((\sim k_2) \lll 11)) \\
k_5 &:= k_5 \oplus k_4 \\
k_6 &:= k_6 + k_5 \\
k_7 &:= k_7 - (k_6 \oplus ((\sim k_5) \ggg 13)) \\
k_0 &:= k_0 \oplus k_7 \\
k_1 &:= k_1 + k_0 \\
k_2 &:= k_2 - (k_1 \oplus ((\sim k_0) \gg 7)) \\
k_3 &:= k_3 \oplus k_2 \\
k_4 &:= k_4 + k_3 \\
k_5 &:= k_5 - (k_4 \oplus ((\sim k_3) \ll 5)) \\
k_6 &:= k_6 \oplus k_5 \\
k_7 &:= k_7 + k_6
\end{aligned}$$

Figure 5.2. The key schedule algorithm *Key_sch*.

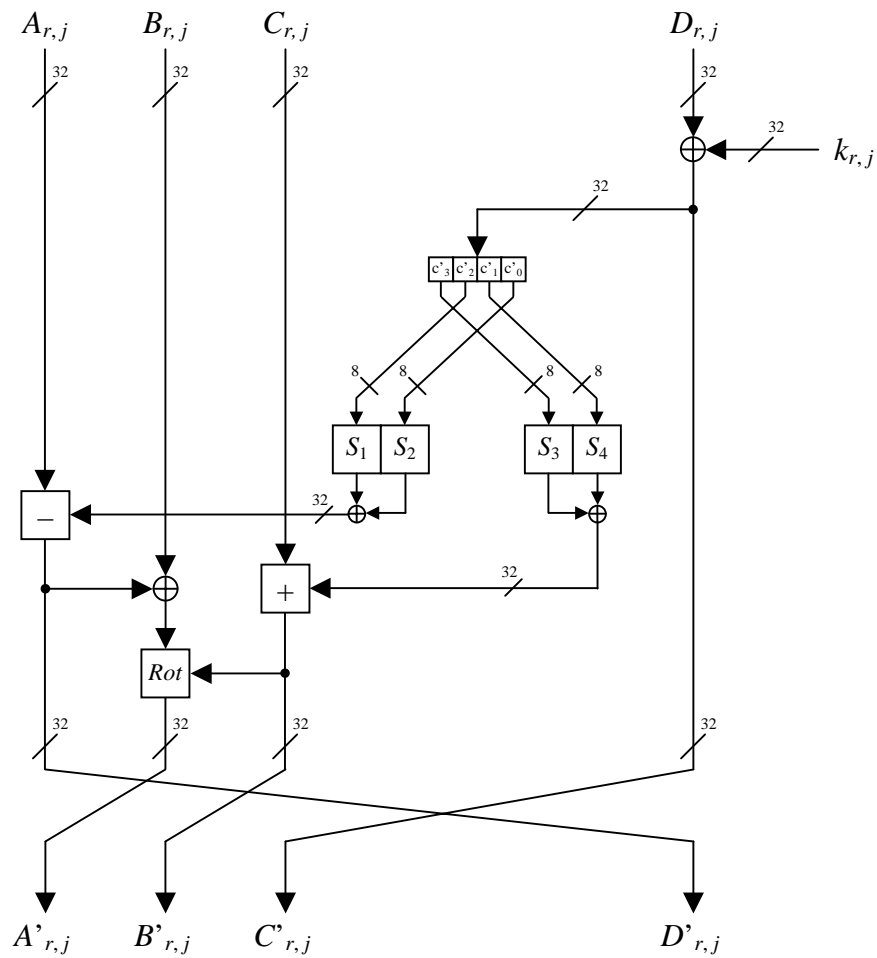


Figure 5.3. The j -th round of the r -th pass of the encryption algorithm.

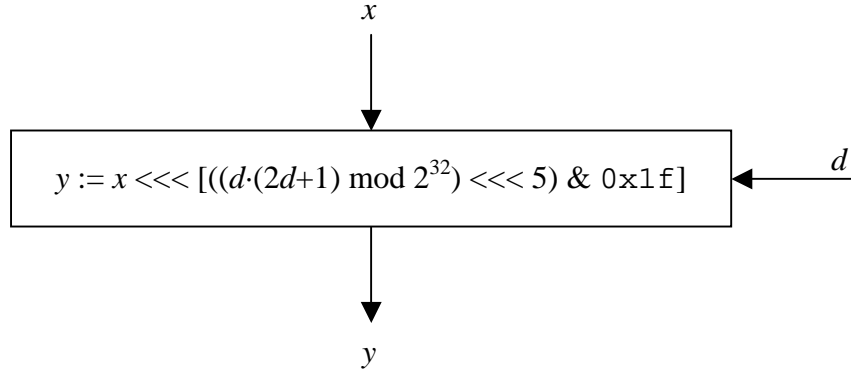


Figure 5.4. The data-dependent rotation function *Rot*.

The TGR decryption algorithm is obtained by taking the inversion of the TGR encryption algorithm (suitable modification of the round function and opposite order of the subkeys).

6 Resistance of TGR to Linear Cryptanalysis

It has been stated in [5] that the best linear approximation of a cipher, satisfied with the probability p_L is bounded as follows:

$$\left| p_L - \frac{1}{2} \right| \leq 2^{\alpha-1} \left| p_\beta - \frac{1}{2} \right|^\alpha, \quad (6.1)$$

where α is the number of S-box linear approximations involved in the linear approximation of the cipher and p_β represents the probability of the best S-box linear approximation (among all the α S-box linear approximations). In every round of the block cipher TGR there are involved two 16×32-bit S-boxes each consisting of two 8×32-bit S-boxes taken from the CAST-256. The linear approximation of a block cipher is based on the assumption of independent round keys such that the linear expressions approximating the S-boxes are independent. The sequence of approximations of the round functions (involving approximations of the S-boxes) results in the overall linear expression for the cipher. According to [6] the number of known plaintexts required to almost sure deduction of some bits of the round keys is approximately equal to

$$N_p = \left| p_L - \frac{1}{2} \right|^{-2}. \quad (6.2)$$

It was shown in [5] (see Lemma 3.3 above) that the probability p_β is given by

$$\left| p_\beta - \frac{1}{2} \right| = \frac{2^{m-1} - NL_{\min}}{2^m}, \quad (6.3)$$

where m is the number of input bits of the S-box and NL_{\min} is minimal nonlinearity of the S-boxes involved in the approximation of the cipher. In our case of TGR cipher we have $m = 16$ and using Theorem 4.4 we have calculated NL_{\min} being 28736 for the 16×32-bit S-box built from the substitution boxes S_1 and S_2 taken from the CAST-256 cipher. The best linear approximation of TGR cipher appears to be constructed using two round characteristics when in each round it is approximated the left one 16×32-bit S-box (see Figure 5.3) and the arithmetic addition and subtraction are replaced by xor operation and the data-dependent rotation is neglected. These characteristics are not iterative ones. When calculating (6.3) with our data we obtain

$$\left| p_\beta - \frac{1}{2} \right| = \frac{63}{1024}$$

and putting $\alpha = 24$ in (6.1) we have

$$\left| p_L - \frac{1}{2} \right| \leq 0.725545 \cdot 10^{-22}.$$

From (6.2) we get that the number of required plaintexts to perform the linear cryptanalysis is

$$N_p \geq 1.8996 \cdot 10^{44} \approx 2^{147}$$

which is much more than the number 2^{128} of all available plaintexts.

If we perform such analysis, when in each two round characteristic there are approximated two 8×32-bit substitution boxes S_1 and S_2 having nonlinearity 74, we get that the required number of plaintexts is greater than 2^{121} . It shows that we obtain the better resistance of the cipher to linear cryptanalysis when considering bigger S-boxes in the round function confirming this way the observation made by Youssef et al. in [11].

Let us consider the TGR cipher reduced to two passes, i.e. 16 rounds. Performing the linear cryptanalysis as described above we get the following data. In the first case of 16×32-bit S-boxes, there are then $\alpha = 16$ S-box linear approximations involved in the approximation of the cipher and it is required more than 2^{98} plaintexts which is an unrealistic amount. In the second case of 8×32-bit S-boxes, there are then $\alpha = 32$ S-box linear approximations involved in the approximation of the cipher and it is required more than 2^{81} plaintexts. We can

conclude that TGR algorithm has a one pass (8 rounds) of the security margin with respect to the linear cryptanalysis.

References

- [1] C. M. Adams, "Constructing Symmetric Ciphers using the Cast Design Procedure", *Designs, Codes, and Cryptography*, vol. 12, no. 3, 1997, pp. 283-316.
- [2] C. M. Adams, "The CAST-256 Encryption Algorithm", available at AES web site: csrc.nist.gov/encryption/aes
- [3] N. Ahmed and K. R. Rao, "Orthogonal Transforms for Digital Processing", Springer-Verlag, 1975.
- [4] R. Anderson and E. Biham, "Tiger: New Hash Function", Third International Workshop, Fast Software Encryption, LNCS 1039, Springer-Verlag, 1996, pp. 89-97.
- [5] J. Lee, H. M. Heys and S. E. Tavares, "On the Resistance of the CAST Encryption Algorithm to Differential and Linear Cryptanalysis", *Designs, Codes, and Cryptography*, vol. 12, no. 3, 1997, pp. 267-282.
- [6] M. Matsui, "Linear Cryptanalysis Method for DES Cipher", *Advances in Cryptology, Proceedings of Eurocrypt '93*, T. Hellesest, Ed., Springer-Verlag, 1994, pp. 386-397.
- [7] W. Meier and O. Staffelbach, "Nonlinearity Criteria for Cryptographic Functions", *Advances in Cryptology, Proceedings of Eurocrypt '89*, LNCS 434, J. -J. Quisquater and J. Vandewalle, Eds., Springer-Verlag, 1990, pp. 549-562.
- [8] K. Nyberg, "Perfect Nonlinear S-Boxes", *Advances in Cryptology, Proceedings of Eurocrypt '91*, LNCS 547, D. W. Davies, Ed., Springer-Verlag, 1991, pp. 378-386.
- [9] J. Pieprzyk and G. Finkelstein, "Towards Effective Nonlinear Cryptosystem Design", *IEE Proceedings-E*, vol. 135, 1988, pp. 325-335.
- [10] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, "The RC6 Block Cipher", available at AES web site: csrc.nist.gov/encryption/aes
- [11] A. M. Youssef, Z.G. Chen and S. E. Tavares, "Construction of Highly Nonlinear Injective S-Boxes with Application to CAST-like Encryption Algorithm", *Proceedings of the Canadian Conference on Electrical and Computer Engineering (CCECE '97)*, pp. 330-333.