Control and Cybernetics

vol. **36** (2007) No. 4

Nonlinearity of the round function

by

Marcin Kontak and Janusz Szmidt

Military University of Technology
Faculty of Cybernetics, Institute of Mathematics and Cryptology
ul. Kaliskiego 2, 00-908 Warsaw, Poland
e-mail: mkontak@wp.pl, j.szmidt@neostrada.pl

Abstract: In the paper we present the results which enable to calculate the nonlinearity of the round function with quite large dimensions, e.g. 32×32 bits, which are used in some block ciphers. It can be used to estimate resistance of these ciphers against linear cryptanalysis. We give the application to linear cryptanalysis of the TGR block cipher.

Keywords: Boolean functions, substitution boxes, Walsh transform, linear cryptanalysis, TGR algorithm.

1. Introduction

The linear cryptanalysis introduced by M. Matsui (1994) is one of the basic 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 Meier and Staffelbach (1990), Nyberg (1991) and Pieprzyk, Finkelstein (1988) is essential in formulation of linear cryptanalysis. In this paper we consider the round function of a block cipher consisting of parallel S-boxes, whose inputs are concatenated and outputs xored giving in this way the output of the round function. The problem is to calculate the nonlinearity of such a 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 (Adams, 1997, 1999) the round function was used 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 Lee, Heys and Tavares (1997). In present, it is not possible to calculate in a direct way the nonlinearity of this round function. In Youssef, Chen and Tavares (1997) the authors stated, without giving details, that they had calculated the nonlinearity and gave the numerical result. Following their suggestions we have given here Theorem 1, making it possible to calculate the nonlinearity of the function. The round function examined is a good approximation of the one used in the cipher CAST-256 (Adams, 1999), where in two cases bitwise addition is replaced by algebraic operations like arithmetic addition and subtraction modulo 2^{32}. The calculation of the nonlinearity of the round function is used to estimate the resistance of the cipher against linear cryptanalysis. The result is better when we consider the round function as a whole than the one obtained by taking into account the nonlinear properties of the individual S-boxes. We show 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 R. Anderson and E. Biham (1996) working in the encryption mode.

2. The nonlinearity of the round function

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

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 $\{-1, 1\}$.

The real function of $\mathbf{u} \in Z_2^m$ defined as $W(f)(\mathbf{u}) = \sum\limits_{\mathbf{x} \in Z_2^m} f(\mathbf{x})(-1)^{\mathbf{u} \cdot \mathbf{x}}$ is called the *Walsh transform* of the function f, where $f : Z_2^m \to \mathbf{R}$. The Walsh transform of the polar function $\hat{f}$ at the point $\mathbf{u}$ is denoted $W(\hat{f})(\mathbf{u})$. For the fast method computing of the Walsh transform see for example Ahmed, Rao (1975).

The *nonlinearity* of a Boolean function $f : Z_2^m \to Z_2$ is defined as $NL_f = \min\limits_{\mathbf{a},c} \#\{\mathbf{x} \in Z_2^m | f(\mathbf{x}) \neq \mathbf{a} \cdot \mathbf{x} \oplus c\}$, where $\mathbf{a} \in Z_2^m, c \in Z_2$.

LEMMA 1 *Let* $f : Z_2^m \to Z_2$, *then* $NL_f = 2^{m-1} - \frac{1}{2} \max\limits_{\mathbf{a} \in Z_2^m} |W(\hat{f})(\mathbf{a})|$.

A *substitution box* (S-box) of dimension $m \times n$ is a transformation $S : Z_2^m \to Z_2^n$, where $m, n \in N$. The substitution box S can be considered as a collection of its coordinates being n Boolean functions, i.e. $S = [f_n, f_{n-1}, \ldots, f_1]$, where $f_i : Z_2^m \to Z_2, i = 1, 2, \ldots, n$.

The *nonlinearity* of substitution box $S : Z_2^m \to Z_2^n$ is defined as $NL_S = \min\limits_{\mathbf{b}} NL_{\mathbf{b} \cdot S}$, where $\mathbf{b} \in Z_2^n \setminus \{\mathbf{0}\}, \mathbf{b} = [b_n, b_{n-1}, \ldots, b_1]$ and $NL_{\mathbf{b} \cdot S}$ is nonlinearity of the Boolean function $\mathbf{b} \cdot S = b_n f_n \oplus b_{n-1} f_{n-1} \oplus \ldots \oplus b_1 f_1$.

For a given substitution box $S : Z_2^m \to Z_2^n$ the *linear approximation table* is defined, whose elements are $LAT_S(\mathbf{a}, \mathbf{b}) = \#\{\mathbf{x} \in Z_2^m | \mathbf{a} \cdot \mathbf{x} = \mathbf{b} \cdot S(\mathbf{x})\} - 2^{m-1}$, where $\mathbf{a} \in Z_2^m, \mathbf{b} \in Z_2^n \setminus \{\mathbf{0}\}$.

LEMMA 2 *For a substitution box* $S : Z_2^m \to Z_2^n$ *one has* $NL_S = 2^{m-1} - \max\limits_{\mathbf{a},\mathbf{b}} |LAT_S(\mathbf{a}, \mathbf{b})|$, *where* $\mathbf{a} \in Z_2^m, \mathbf{b} \in Z_2^n \setminus \{\mathbf{0}\}$.

By the *linear approximation* of a substitution box $S : Z_2^m \to Z_2^n$ 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 for given $\mathbf{a}$ and $\mathbf{b}$, it is

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

Then

$$\left| p - \frac{1}{2} \right| = \frac{|LAT_S(\mathbf{a}, \mathbf{b})|}{2^m}$$

has a meaning of efficiency of the linear approximation of substitution box $S : Z_2^m \to Z_2^n$. Let p_β denote the probability of the best linear approximation, i.e. the one, for which the efficiency $|p_\beta - \frac{1}{2}|$ has the biggest value.

Lemma 3 (Lee, Heys and Tavares, 1997) *For a substitution box $S : Z_2^m \to Z_2^n$ there is*

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

Let $F : Z_2^{km} \to Z_2^n$ be a transformation such that $F(\mathbf{x}) = F(\mathbf{x}_k, \mathbf{x}_{k-1}, \ldots, \mathbf{x}_1) = S_1(\mathbf{x}_1) \oplus S_2(\mathbf{x}_2) \oplus \ldots \oplus S_k(\mathbf{x}_k)$, where $S_i : Z_2^m \to Z_2^n, i = 1, 2, \ldots, k$ and $S_i = [f_{i,n}, f_{i,n-1}, \ldots, f_{i,1}], f_{i,j} : Z_2^m \to Z_2, j = 1, 2, \ldots, n$ (see Fig. 1).

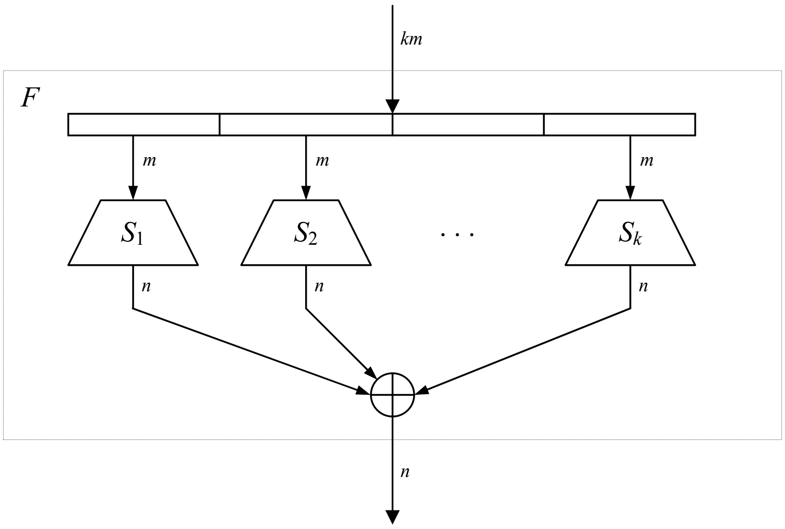

Figure 1. The structure of F round function.

Similarly to that of the substitution boxes we define the nonlinearity of the transformation $F : Z_2^{km} \to Z_2^n$:

$$NL_F = \min_{\mathbf{b}} NL_{\mathbf{b}\cdot F}, \tag{1}$$

where $\mathbf{b} \in Z_2^n \setminus \{\mathbf{0}\}, \mathbf{b} = [b_n, b_{n-1}, \ldots, b_1], F = [F_n, F_{n-1}, \ldots, F_1], F_j : Z_2^{km} \to Z_2, F_j(\mathbf{x}) = F_j(\mathbf{x}_k, \mathbf{x}_{k-1}, \ldots, \mathbf{x}_1) = f_{1,j}(\mathbf{x}_1) \oplus f_{2,j}(\mathbf{x}_2) \oplus \ldots \oplus f_{k,j}(\mathbf{x}_k)$ and $NL_{\mathbf{b}\cdot F}$ is the nonlinearity of the Boolean function $\mathbf{b}\cdot F = b_n F_n \oplus b_{n-1} F_{n-1} \oplus \ldots \oplus b_1 F_1$.

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

3. The TGR algorithm

The TGR algorithm is a block cipher, which works on 128-bit blocks and uses 256-bit keys. 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 ($j = 0, 1, \ldots, 7$).

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 input the main key $K = (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7)$ and gives as 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 input to Key_sch the key K_1 and we get as 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 Fig. 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 left and right shifts, 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 $(A'_{r,j}, B'_{r,j}, C'_{r,j}, D'_{r,j})$. The structure of the round is depicted in Fig. 3. The S-boxes S_1, S_2, S_3, S_4 are taken from the CAST-256 cipher (Adams, 1999) and operation Rot is the data-dependent rotation function

$$Rot(x, d) = x \lll [(((d(2d+1) \bmod 2^{32}) \lll 5)\ \&\ 0x1f],$$

taken from the RC6 cipher (Rivest et al., 2001), where & is logical AND operation.

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). The TGR design is based on the hash function *Tiger* proposed by R. Anderson and E. Biham (1996).

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

where the constant $c = 0xa5a5a5a5$.

Figure 2. The key schedule algorithm *Key_sch*.

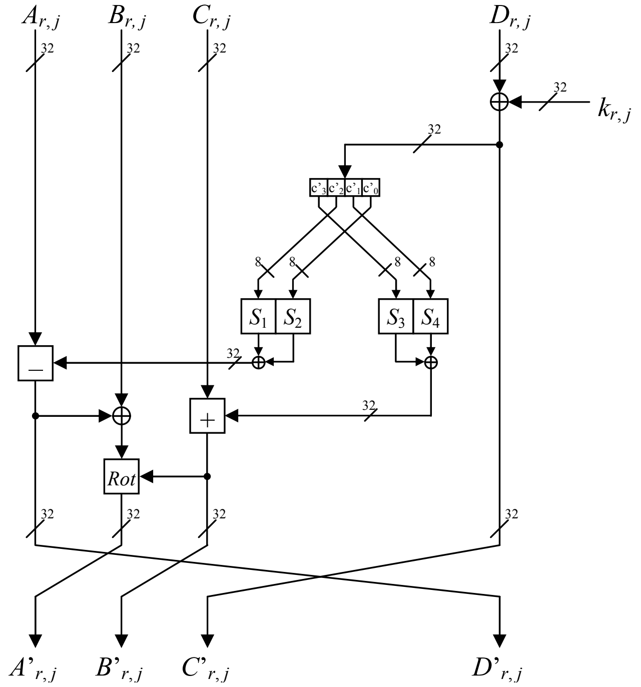

Figure 3. The j-th round of the r-th pass of the encryption algorithm.

4. Resistance of TGR to linear cryptanalysis

It has been stated in Lee, Heys and Tavares (1997) that the best linear approximation of a cipher, satisfied with the probability p_L is bounded as follows:

$$\left|p_L - \frac{1}{2}\right| \leq 2^{\alpha-1}\left|p_\beta - \frac{1}{2}\right|^\alpha, \tag{2}$$

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 two 16×32-bit S-boxes are involved 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 Matsui (1994) the number of known plaintexts required for an almost sure deduction of some bits of the round keys is approximately equal to

$$N_p = \left|p_L - \frac{1}{2}\right|^{-2}. \tag{3}$$

It was shown in Lee, Heys and Tavares (1997) (see Lemma 3 above) that the probability p_β is given by

$$\left|p_\beta - \frac{1}{2}\right| = \frac{2^{m-1} - NL_{\min}}{2^m}, \tag{4}$$

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 formula (1) and Theorem 1 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 2-round characteristic when in each round it is approximated by the left one 16×32-bit S-box (see Fig. 3) and the arithmetic addition and subtraction are replaced by xor operation and the data-depended rotation is neglected. This characteristic is not iterative one. When calculating (4) with our data we obtain

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

and putting $\alpha = 24$ in (2) we have

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

From (3) 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 that the number 2^{128} of all available plaintexts.

If we perform such analysis, when in each two round characteristic two 8×32-bit substitution boxes S_1 and S_2 are approximated having nonlinearity 74, we get that the required number of plaintexts is greater than 2^{121}. It shows that we obtain the better estimation of resistance of the cipher to linear cryptanalysis when considering bigger S-boxes in the round function, confirming thereby the observation made by A. M. Youssef, Chen and Tavares (1997).

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 more than 2^{98} plaintexts are required. 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 more than 2^{81} plaintexts are required. We can conclude that TGR algorithm has a security margin with respect to the linear cryptanalysis.

References

Adams, C.M. (1997) Constructing Symmetric Ciphers Using the CAST Design Procedure. *Design, Codes, and Cryptography* **12** (3), 283-316.

Adams, C.M. (1999) The CAST-256 Encryption Algorithm. Available at AES web site: `csrc.nist.gov/encryption/aes`

Ahmed, N. and Rao, K.R. (1975) *Orthogonal Transforms for Digital Processing.* Springer-Verlag.

Anderson, R. and Biham, E. (1996) Tiger: New Hash Function. *Third International Workshop. Fast Software Encryption.* **LNCS 1039**. Springer-Verlag, 89-97.

Lee, J., Heys, H.M. and Tavares, S.E. (1997) On the Resistance of the CAST Encryption Algorithm to Differential and Linear Cryptanalysis. *Design, Codes, and Cryptography* **12** (3), 267-282.

Matsui, M. (1994) Linear Cryptanalysis Method for DES Cipher. In: T. Helleseth, ed., *Advances in Cryptology. Proceedings of Eurocrypt'93.* **LNCS 765**. Springer-Verlag, 386-397.

Meier, W. and Staffelbach, O. (1990) Nonlinearity Criteria for Cryptographic Functions. In: J. -J. Quisquater and J. Vandewalle, eds., *Advances in Cryptology. Proceedings of Eurocrypt'89* **LNCS 434**. Springer-Verlag, 549-562.

Nyberg, K. (1991) Perfect Nonlinear S-Boxes. In: D.W. Davies, ed., *Advances in Cryptology. Proceedings of Eurocrypt'91.* **LNCS 547**. Springer-Verlag, 378-386.

PIEPRZYK, J. and FINKELSTEIN, G. (1988) Towards Effective Nonlinear Cryptosystem Design. *IEE Proceedings-E* **135**, 325-335.

RIVEST, R.L. , ROBSHAW, M.J.B., SIDNEY, R. and YIN, Y.L. (2001) The RC6 Block Cipher. Available at AES web site: `csrc.nist.gov/encryption/aes`

YOUSSEF, A.M., CHEN, Z.G., and TAVARES, S.E. (1997) 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)*, 330-333.