International Journal of Engineering & Technology, 7 (3.27) (2018) 120-124

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Linear Cryptanalysis of S-Box BRADG

Emaan Oudha Oraby[1*], Salah A.K. Albermany[2]

[1]*Faculty of Computer Science and Mathematics, Mathematics Department, Iraq.*
[2]*Faculty of Computer Science and Mathematics, Mathematics Department, Iraq*

Abstract

Block cipher reaction automata direct graph (BRADG) is used in protection wireless networks. BRADG processes data blocks of B bits with key length of B bits and given ciphertext of size B bits, where B is 64,128,512,...bits. BRADG is a faster and more efficient way to encrypt large data compared with the previous design of block cipher. In this thesis, the researcher presented a study to attack for BRADG algorithm by using linear cryptanalysis technique, by known-plaintexts and corresponding of the ciphertexts. As the results, it's possible to break: one bit in subkey 1-state BRADG cipher with at least 2 to power 3known-plaintext, and 16 bits subkey 1-state BRADG cipher with 2 to power 24 known plaintexts. The success rate of each attack is 84% , 92% ,97% and 99% depending on the number of known plaintext and the probability that the equation of the best approximation holds.

1. Introduction

Linear cryptanalysis is first introduced by Mitsuru Matsui in [1]. The cryptanalyst endvours to find a linear equation x1 ⊕ . . . ⊕ xi = y1 ⊕ . . . ⊕yj in the input and output bits of some segment of the cipher which matches truly with possibility and adequately different to 0.5. “Sufficiently different” which denotes that for a familiar-plaintext attack on attainable number of known plaintexts, at the time when the right key (or part of it) is tested on all of these known plaintexts, the number of plaintexts for them the equation maintains, and will divert remarkably from a half of the entire value. The equation like this type is a familiar one that is “linear approximation” linear cryptanalysis is a common structure of cryptanalysis established on getting affine approximations of the activity of a cipher. Attacks have been developed for blocking ciphers and stream ciphers. Linear cryptanalysis is one of the two nearly almost prominently utilized attacks on block ciphers.

The exploration is ascribed to Matsui, that basically used the expertise of the FEAL cipher (Matsui and Yamagishi [1] At a subsequent time, Matsui produced an attack on the Data Encryption Standard (DES), consequently ushering the earlier empirical cryptanalysis of the cipher mentioned in the open community (Matsui, 1993)[1]. The attack on DES is not commonly practical, and demanding 2^{47} known plaintexts. • Nyberg [2], and Harpes, Kramer and Massey [3] have implemented analyses that yielded in that some of Matsui’s suppositions were overly despairing, and that proper complication of the attack would sounds more exquisite than as he once anticipated (despite the fact that new complexity equations are not supplied.) • Junod [4] furnished prove that the time demanded by Matsui’s attack was actually equal just to that necessary to carry out 241 DES encryptions. • Biryukov et al [5], directing study on the usage of many linear approximations concurrently (Matsui’s attack utilized two) speculated that the attack’s space demands that might be decreased up to 241 consulting a specified set of 108 approximations. (They do not seem to have successfully implemented this attack, however.) They also conjectured that, although fresh techniques would be demanded, using approximately 10,000 approximations simultaneously would lessen the space requirements to 236.

Salah Albermany et al. in the year 2014, and Fatima R.H. AL. Kalidi where they propose a novel design, that is, block cipher keys, by attempting to develop certain algorithm which progresses the RADG method to the BRADG block cipher key while maintaining the RADG properties. BRADG (block cipher reaction automata direct graph) is utilized for supplying effective protection to the wireless networks. BRADG is situated on the unbalanced Feistel structure in both encryption and decryption. [6],[8].

Generally, the security of a block cipher is founded after voluminous analysis of its resistance to branch out cryptanalytic attacks particularly by some ways of heuristic study of its mathematical characteristics, hoping to find short-cut attacks that bespeak the shortcoming of the design. This study is ultimately known as Linear cryptanalysis of BRADG block cipher. A block cipher is recognized and confirmed as “secure” by the cryptology group, when showing opposition to most familiar cryptanalytic attacks, its confidence security develops when it represent an optimal resistance over a part of time, normally by a considerable number of year's issues, even against progress in crypt analyses that were not beforehand thought of. **[7].**

2. Related Work

In [8] producing a new approach for cryptanalysis of DES cipher, such approach has enabled us in the first known-plaintext attack of the full 16-round DES cipher and the starting pace towards the only-ciphertext attack, and to dip further deeply into the only-ciphertext attack. In [9] presented the essential notions of linear and differential cryptanalysis as applicable to a basic Cipher. In [10] presenting the solutions for the two open problems by using Matsui's Algorithm 2 with multiple linear approximations posed earlier by Biryukov, De Canniere and M. Quisquater at Crypto'04. [11] They proposed multivariate linear cryptanalysis as modern approach for using multiple linear approximations. It is based on a multivariate statistical model and permits realistic key equivalence and wrong key randomization hypotheses without introducing

extra restrictive assumptions about the distributions of the correlations of the utilized linear approximations. In that [12] they improve the Multidimensional linear cryptanalysis of block ciphers, by introducing a number of new ideas. In [13],[2] implementing analyses which display that some of Matsui's Despite the fact that new approximation estimates are not made available. In [3] afforded a demonstration that the period of time needed by Matsui's attack was actually equal only to that necessary to perform 2^{41} DES encryptions. In [4] running a study on the use of many linear approximations simultaneously (Matsui's attack had used two) conjectured that the attack's space requirements could be reduced to 2^{41} by utilizing a definite set of 108 approximations.
Implementation of BRADG and the results shown that the humming distance between individual cipher text differ significantly code breaking depend on classical cryptography.[6]

3. Theoretical Background

BRADG Design

A new design of the RADG block cipher key, shown in Figure (2.3), consists of round function based on the unbalanced Feistel structure, which divides the input block into two halves (L_0 and R_0) that are not equal in size, such that the size of left half L_0 and right half R_0 will be: L_0 = x /2 bits, R_0= x bits

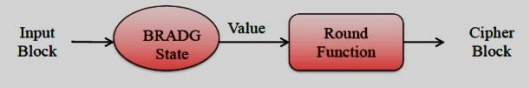

Figure 3.1: General design of BRADG encryption

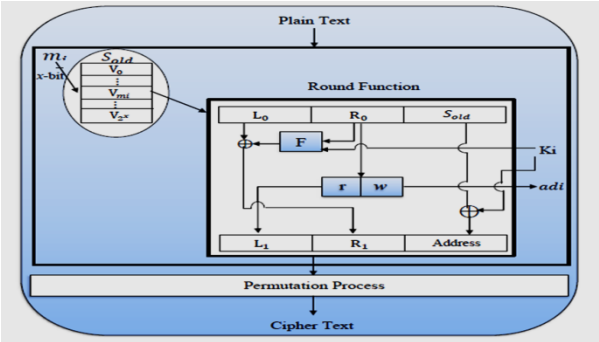

Figure 3.2: Round encryption process

From Figure (3.2), output of the encryption process using the BRADG design consists of two parts. The first part represents the cipher text of input block x, denoted by cipher text C, while the second part represents the cipher text of address state Sold, denoted by cipher address. The address Sold of the RADG state is ciphered by adding it to the equal number of key bits (ad bits) taken from the left half of the sub key in order to get the address cipher. This address cipher is used in the decryption process to get the address number of states, is used to encrypt a certain input block. If the address in the R set (reaction state), in this case, onemust encrypt the address of the J state, which causes the random case in those states of the R set. If the address belongs to the J state in decryption process, this means that the address returns to the state in the R set; in this [6],[8]

Round Function (RF) Algorithm

Input: The value V of BRADG design state, the Key K of size $2x$ bits
Output: Cipher Text B
Step 1: $V \rightarrow L_0$, R_0
Step 2: $R_1 \leftarrow L_0 \oplus F$ (R_0, KL)
Step 3: r, $w \leftarrow R_0$
Step 4: $L_1 \leftarrow r$
Step 5: $S_{new} \leftarrow w$
Step 6: k_{LL}, $k_{LR} \leftarrow K_L$
Step 7: $address \leftarrow S_{old} \oplus k_{LL}$
Step 8: R_1, L_1, $Address \rightarrow B$
Step 9: $returnB$

BRADG Encryption and Decryption Algorithm

One can perform encryption and decryption by using BRADG algorithm [8].

4. Proposed Design

Linear Cryptanalysis

Linear cryptanalysis tries to consume a big likelihood of occurrences of linear terms involving plaintext bits, "ciphertext" bits (actually the researcher will employ bits from the 2nd last round output), and subkey bits. It is a well-known plaintext attack: that is, it is premised on the attacker getting information on a set of plaintexts and the equivalent ciphertexts. Nevertheless, the attacker does not have any way to choose which plaintexts (and equivalent ciphertexts) are obtainable. In many applications and scenarios, it is satisfactory to undertake that the attacker has understanding of a random set of plaintexts and the equivalent cipher texts. [5]
The essential notion is to comply with the operation of a portion of the cipher with a term that is linear where the linearity relegates to a mod-2 bit-wise operation (i.e., exclusive-OR indicated by "⊕"). Such a term is of the form:

$$X_{i_1} \oplus X_{i_2} \oplus \ldots \oplus X_{i_u} \oplus Y_{j_1} \oplus Y_{j_2} \oplus \ldots \oplus Y_{j_v} = 0 \qquad (1)$$

where X_i displays the i-th bit of the input X = [X_1, X_2, ...] and Y_j represents the j-th bit of the output Y = [Y_1, Y_2, ...]. This balance is depicting the exclusive-OR "sum" of u input bits and v output bits [11] .
The attempt in linear cryptanalysis is to determine the terms of the form above which have a high or low likelihood of presence. (No clear linearity such as above shall hold for all input and output values or the cipher would be in a trivial way very slight.) If a cipher displays a tendency for equation (1) to hold with high likelihood or not hold with high likelihood, this is proof of the cipher's poor randomization capabilities. Assume that if one randomly chose values for u + v bits and located them into the equation above, then the likelihood that the expression would hold would be approximately 1/2. It is the deviation or bias from the probability of 1/2 for an expression to hold that is used in linear cryptanalysis: the further away that a linear expression is from holding with a likelihood of 1/2, the better the cryptanalyst is capable to implement linear cryptanalysis. In the remnant of the paper, relegate to the amount by which the probability of a linear expression having deviates from 1/2 as the linear probability bias. Hence, if the expression above has with probability p_L for randomly chosen plaintexts and the equivalent ciphertexts, then the probability bias is $p_L - 1/2$. The greater the magnitude of the probability bias, $|p_L - 1/2|$, the better the applicability of linear cryptanalysis with fewer known plaintexts needed in the attack [11]

Notations and Preliminaries

Figure (4.1) show a data randomization part of **BRADG** cipher. omit the expansion function and S-boxes otherwise indicated. The following notations are used throughout this paper, where the right mist bit is referred to as the zero-th bit.

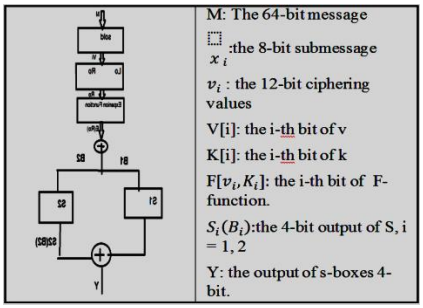

Figure 4.1: BRAD cipher (part)

Definition

Suppose for given S-Box Fatima [8] and albermany [6] S_i(i=1,2), $1 \leq \propto \leq 255$ and $1 \leq \beta \leq 15$, let defiend $NS_i(\propto,\beta)$ as the number of times out of 256 input patterns of Sa, Such that an XORed value of the input bits masked by $\propto$ coincides with an XORed value of the output bits masked β, where the $\propto$ is size of input to s-box and the β is the size of output of s-box ,that is say
$NS_i(\propto,\beta) = \neq$
$\{u/0 \leq u \leq 256, (\oplus_{s=0}^{7} u[s].\propto [s])\} = (\oplus_{t=0}^{3}(s_a(u))[t].\beta[t]))\}$
(3.1)[14][15]
Where the symbol **(.)** denoted a bitwise AND operation.

Algorithm to Find Probability and Bais of Linear Expression

Input : $sboxes$, alpha , beta.
Step 1:for each alpha 1-255
Step 2: for each beta 1-15
Step 3: for x←0 to 255
step 4: t_1←convert to binary (x)
Step 5:t_2←convert to binary (alpha)
Step 6: t_3← t1 ∧ t2
Step 7:t4←sum (XoR(T3))
Step 8: left side (i,1)←t_4
Step9:tt_1← convert to binary (beta)
Step10: row← select bit (1278)
Step11: column← select bit (3456)
Step 12 :ts←findsbox value (row, column)
step 13:tt_3← ts ∧ tt_1
Step 14 :right side (i,1) ← sum(XOR(tt_3))
Step 15: next x
Step 16: bias (alpha, beta) ← sum (left side, right side)
Step 17: bias (alpha, beta) ←bias-128
Step 18 :next beta
Step 19:next alpha
Step 20:pr←bias (alpha ,beta)/256.

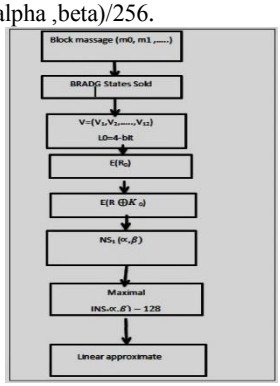

Figure 4.2: Linear approximation of s-boxes

Table 4.1: A Distribution Table of S_1 (part)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	12	-10	-4	-6	4	2	-14	12	10	-4	-6	0	-2	4
0	-2	2	2	6	-8	16	-4	4	2	-18	10	-18	-24	0
4	2	-2	0	-4	-22	-18	-6	2	-4	20	-14	2	4	4
-6	0	-2	2	12	6	-4	0	-2	-12	-2	2	8	2	-4
-2	0	-26	-4	-2	0	2	-10	-4	-6	8	-10	0	-2	-8
0	-2	-6	2	6	-8	-8	0	0	14	10	6	2	12	4
0	-10	-10	0	-8	-2	6	-2	2	-4	8	-10	2	4	-8
14	-12	22	6	-4	-2	0	0	-14	8	6	6	8	-6	0
6	8	-10	8	-6	-12	6	-2	-12	-6	-8	2	-12	2	4
-4	2	2	-2	6	0	-4	-8	-4	2	-6	-6	18	4	0
-4	2	-2	4	0	6	-14	-10	6	0	-8	-6	-6	-4	4
26	-8	-2	6	-16	-6	-8	-4	2	-8	2	2	0	2	12
2	-12	-2	8	-2	8	-2	2	4	2	-4	14	4	10	0
4	-2	6	-6	-6	-8	-20	0	-4	14	-18	14	-2	-20	-48
4	-2	2	0	12	-2	10	-2	6	4	4	-2	-2	-4	4
-6	4	2	-2	0	-2	-4	0	14	8	2	6	4	2	4
-6	0	10	0	-18	12	2	6	8	10	-4	2	8	2	0
0	2	-2	6	-6	0	16	0	0	10	-10	-6	-10	12	-12
0	-14	2	4	4	-2	14	-2	2	-8	4	10	-2	20	0
-2	0	-22	-2	-4	2	-12	12	6	16	-2	2	4	2	0
-2	-4	-6	0	10	0	2	-6	0	2	-8	-18	0	-6	4
0	2	6	-2	2	8	0	-4	4	-2	-6	6	-6	0	-8
-4	-2	2	4	0	-6	-2	2	-14	0	0	-2	-2	-4	-4
2	-20	-6	18	-4	-14	0	-4	-6	12	-18	6	4	2	-4

Table 4.2: A Probability Table of s1 (part)

0.507813	0.546875	0.460938	0.484375	0.476563	0.515625	0.507813	0.445313	0.546875	0.539063	0.484375	0.476563	0.500000	0.492188	0.515625
0.500000	0.492188	0.507813	0.507813	0.523438	0.468750	0.562500	0.484375	0.515625	0.507813	0.429688	0.539063	0.429688	0.40625	0.500000
0.515625	0.507813	0.492188	0.500000	0.484375	0.414063	0.429688	0.476563	0.507813	0.484375	0.578125	0.445313	0.507813	0.515625	0.515625
0.476563	0.500000	0.492188	0.507813	0.546875	0.523438	0.484375	0.500000	0.492188	0.453125	0.492188	0.507813	0.531250	0.507813	0.484375
0.492188	0.500000	0.398438	0.484375	0.492188	0.500000	0.507813	0.460938	0.484375	0.476563	0.531250	0.460938	0.500000	0.492188	0.468750
0.500000	0.492188	0.476563	0.507813	0.523438	0.468750	0.468750	0.500000	0.500000	0.554688	0.539063	0.523438	0.507813	0.546875	0.515625
0.500000	0.460938	0.460938	0.500000	0.468750	0.492188	0.523438	0.492188	0.507813	0.484375	0.531250	0.460938	0.507813	0.515625	0.468750
0.554688	0.453125	0.585938	0.523438	0.484375	0.492188	0.500000	0.500000	0.445313	0.531250	0.523438	0.523438	0.531250	0.476563	0.500000
0.523438	0.531250	0.460938	0.531250	0.476563	0.453125	0.523438	0.492188	0.453125	0.476563	0.468750	0.507813	0.453125	0.507813	0.515625
0.484375	0.507813	0.507813	0.492188	0.523438	0.500000	0.484375	0.468750	0.484375	0.507813	0.476563	0.476563	0.570313	0.515625	0.500000
0.484375	0.507813	0.492188	0.515625	0.500000	0.523438	0.445313	0.460938	0.523438	0.500000	0.468750	0.476563	0.476563	0.484375	0.515625
0.601563	0.468750	0.492188	0.523438	0.437500	0.476563	0.468750	0.484375	0.507813	0.468750	0.507813	0.507813	0.500000	0.507813	0.546875
0.507813	0.453125	0.492188	0.531250	0.492188	0.531250	0.492188	0.507813	0.515625	0.507813	0.484375	0.554688	0.515625	0.539063	0.500000
0.515625	0.492188	0.523438	0.476563	0.476563	0.468750	0.421875	0.500000	0.484375	0.554688	0.429688	0.554688	0.492188	0.421875	0.312500
0.515625	0.492188	0.507813	0.500000	0.546875	0.492188	0.539063	0.492188	0.523438	0.515625	0.515625	0.492188	0.492188	0.484375	0.515625
0.476563	0.515625	0.507813	0.492188	0.500000	0.492188	0.484375	0.500000	0.554688	0.531250	0.507813	0.523438	0.515625	0.507813	0.515625
0.476563	0.500000	0.539063	0.500000	0.429688	0.546875	0.507813	0.523438	0.531250	0.539063	0.484375	0.507813	0.531250	0.507813	0.500000
0.500000	0.507813	0.492188	0.523438	0.476563	0.500000	0.562500	0.500000	0.500000	0.539063	0.460938	0.476563	0.460938	0.546875	0.453125
0.500000	0.445313	0.507813	0.515625	0.515625	0.492188	0.554688	0.492188	0.507813	0.468750	0.515625	0.539063	0.492188	0.578125	0.500000
0.492188	0.500000	0.414063	0.492188	0.484375	0.507813	0.453125	0.546875	0.523438	0.562500	0.492188	0.507813	0.515625	0.507813	0.500000
0.492188	0.484375	0.476563	0.500000	0.539063	0.500000	0.507813	0.476563	0.500000	0.507813	0.468750	0.429688	0.500000	0.476563	0.515625
0.500000	0.507813	0.523438	0.492188	0.507813	0.531250	0.500000	0.484375	0.515625	0.492188	0.476563	0.523438	0.476563	0.500000	0.468750
0.484375	0.492188	0.507813	0.515625	0.500000	0.476563	0.492188	0.507813	0.445313	0.500000	0.500000	0.492188	0.492188	0.484375	0.484375
0.507813	0.421875	0.476563	0.570313	0.484375	0.445313	0.500000	0.484375	0.476563	0.546875	0.429688	0.523438	0.515625	0.507813	0.484375

Linear Crypto Analysis of S-Box BRADG

Input: Number of plaintext of states, NoCipherText ,Values of states, SBoxof BRADG, StateAdress.
Output: KeyBit of BRADG
Step 1: select random value of BRADG design denoted by v table
Step 2: select SBoxtable
Step 3: for i←1 to length(PlainText)
Step 4: LR←select plaintext (i)of size 12 bit
Step 5: Lo←LR(1 to 4)
Step 6: Ro←LR(5 to 12)
Step 7:tx←expansion function of (R0) see figure 3.7 in [8]
Step 8 : T1←Tx(1 to 8), T2=Tx(9,16)
Step 9 : Trow←Concatinate(T1(1 to 2),T1(7 to 8))
Step 10: Tcol← T1(3 to 6)
Step 11: Ts← ConvertToBinary(SBox1(Trow,Tcol))
Step 12: Tk← Xor(Ts, Tx(4))
Step 13: Kp(i) ← Tk
Step 14: If Tk← 0 then Nunber of Zero=Number of Zero+1
Step 15: Next i
Step 16:if Number of Zero> (Number of PlainText /2) Then
Step 17: If MinProb>1/2 then
Step 18: KeyBit = 0
Step 19: Else
Step 20: KeyBit = 1
Step 21: End if

Step 22: else
Step 23: If MinProb>1/2 then
Step 24: KeyBit = 1
Step 25: else
Step 26: Key Bit = 0
Step 27: End if
Step 28: End if
Step 29**:** End algorithm

5. Experiment Result

Parameter Information

N = 29 Subkey = K = 0100111001001000[8]
Actual K [4] = Table (4,2) the result of linear cryptoanalysis $N = 29, i = 4, \bar{\imath} = 4$

T=14 <29/2, Key(4) =0

Ro[1,2,3..8] Input									R[4]		Y[1,2..4] Output					Linear Approximation K[4]
1	0	0	1	0	0	0	1		1		0	0	1	1		1
1	0	0	1	0	0	0	1		1		0	0	1	1		1
0	1	1	0	0	0	0	1		0		1	1	0	0		0
1	0	0	0	0	0	0	1		0		1	0	0	1		0
1	0	0	0	0	0	0	1		0		1	0	0	1		0
0	1	0	0	0	0	0	1		0		0	1	0	0		1
1	0	1	1	0	0	0	1		1		1	1	0	0		1
1	1	0	0	0	0	0	1		0		1	0	1	0		0
1	0	1	0	0	0	0	1		0		0	1	0	0		1
1	1	1	1	0	0	0	1		1		0	0	0	1		0
0	0	1	0	0	0	0	1		0		0	0	1	0		1
1	0	0	1	0	0	0	1		1		0	0	1	1		1
1	1	1	0	0	0	0	1		0		0	1	1	1		1
1	1	1	1	0	0	0	1		1		0	0	0	1		0
0	0	0	1	0	0	0	1		1		1	1	1	0		0
1	1	0	0	0	0	0	1		0		1	0	1	0		0
1	1	1	0	0	0	0	1		0		0	1	1	1		1
1	1	1	0	0	0	0	1		0		0	1	1	1		1
1	1	1	1	0	0	0	1		1		0	0	0	1		0
0	1	0	1	0	0	0	1		1		1	0	1	1		0
1	0	1	0	0	0	0	1		0		0	1	0	0		1
0	0	0	1	0	0	0	1		1		1	1	1	0		0
0	1	0	0	0	0	0	1		0		0	1	0	0		1
0	1	0	1	0	0	0	1		1		1	0	1	1		0
0	1	0	0	0	0	0	1		0		0	1	0	0		1
0	0	1	0	0	0	0	1		0		0	0	1	0		1
1	0	0	0	0	0	0	1		0		1	0	0	1		0
1	1	1	1	0	0	0	1		1		0	0	0	1		0
1	0	1	1	0	0	0	1		1		1	1	0	0		1

The Success Rate

N	8	15	29	57
P	0.3125	0.3125	0.3125	0.3125
Success Rate	84%	92%	97%	99%

6. Discussion

Analysis of block cipher cryptosystems using linear cryptanalysis technique depends on the linear approximation of the nonlinear functions used in the design of these systems. That's the weakness of the design for BRADG algorithm, lies in the design of the nonlinear functions F-dependent explanation processes and S-boxes. Where the linear approximation of the function F was found, The researcher design by building a statistical linear route between input and output bits of each S-box, and expand this path to the whole algorithm, and finally reach a linear rough explanation without any intermediate value. The experiments are achieved with MATHLAP software.

7. Conclusion

This linear cryptanalysis for BRADG algorithm satisfies the following:

- It is clear that the increase of plaintext also increase the success rate our method.
- Have completely determined the best linear approximate explanation and it is probability for BRADG algorithm and applied this method to a known-plaintext attack.
- The experimental results have shown that the linear cryptanalysis of BRADG has a far lower complexity.
- The results helps in lowering the amount of computational steps required for an exhaustive key search.
- The probability of success depends greatly on the amount of plaintexts.

References

[1] Matsui M, "Linear cryptanalysis method for DES cipher", Advances in Cryptology-Eurocrypt '93, volume 765 of Lecture Notes in Computer Science, (1993), 386–397.

[2] Nyberg K, "Linear approximation of block ciphers", Advances in Cryptology-Eurocrypt '94, volume 950 of Lecture Notes in Computer Science, (1994), pp. 439–444.

[3] Harpes C, Kramer GG & Massey J, "A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma", Advances in Cryptology-Eurocrypt '95, volume 921 of Lecture Notes in Computer Science, (1995), pp.24–38.

[4] Junod P, "On the complexity of Matsui's attack", Proceedings of the 8th Annual International Workshop on Selected Areas in Cryptography, (2001), pp.199–211.

[5] Biryukov A, De Canni`ere C & Quisquater M, "On multiple linear approximations", Advances in Cryptology-Crypto, volume 3152 of Lecture Notes in Computer Science, (2004), 1–22.

[6] Albermany SA & Safdar G, "Keyless Security in Wireless Network", Springs science and Business Media Network, (2014).

[7] Lei W, "Analysis if iterated block ciphers", Nanyang T. University, (2012).
[8] Fatima R.H. AL Kalidi, "Proposed Design of Reaction(RADG) Block Cipher," Mec. Thesis, University of Luca, Iraq, 2017.
[9] Surendar, A., Samavatian, V., Maseleno, · Andino, Ibatova, A. Z., & Samavatian, · Majid. (n.d.). Effect of solder layer thickness on thermo-mechanical reliability of a power electronic system. Journal of Materials Science: Materials in Electronics, 0, 3. https://doi.org/10.1007/s10854-018-9667-y
[10] Heys HM, "A tutorial on linear and differential cryptanalysis", cryptologia, Taylor and Francis, (2002).
[11] Semacv I, "New Results in the linear cryptanalysis of DES", IACR cryptology e-print archive, (2014).
[12] Bogdanov A, Tischhauser E & Vejre PS, "Multivariate linear cryptanalysis: The past and future of PRESENT", IACR cryptology eprint, (2016).
[13] Fauskanger S & Semacy I, "Separable statistics and multidimensional linear cryptanalysis", eprint.iacr.org, (2017).
[14] Z Iskakova, M Sarsembayev, Z Kakenova (2018). Can Central Asia be integrated as asean? Opción, Año 33. 152-169.
[15] G Cely Galindo (2017) Del Prometeo griego al de la era-biós de la tecnociencia. Reflexiones bioéticas Opción, Año 33, No. 82 (2017):114-133