IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Special Issue-1 E-ISSN: 2347-2693

Measuring the Diffusion Characteristic of Block Ciphers: The Bit Relationship Test (BRT)

Dipanjan Bhowmik[1*], Avijit Datta[2], Sharad Sinha[3]
[1,3]Dept. of Computer Science and Application, University of North Bengal
[2]Dept. of Computer Application, Siliguri Institute of Technology, Siliguri

Abstract- The paper describes a test aimed at measuring the diffusion characteristic of block ciphers. Cryptographic strength of a cipher is directly proportional to the extent to which diffusion is achieved by the underlying cipher, which is measured using the test described in the paper. The paper also enlists the results obtained from the test on various block ciphers. The test algorithm described in the paper will be subsequently added as part of the already existing varied test suite to act as a distinguisher based on the diffusion characteristic of the underlying cipher.

Keywords: Diffusion, Bit-by-bit Successful Matches, Block Cipher, Randomness

I. INTRODUCTION

In order to analyze the strength of a block cipher, various tests are conducted on it [3]. In particular, two fundamental aspects of the block cipher, namely "confusion" and "diffusion" are analyzed. While confusion determines whether there is some sort of linearity in the input and the output, diffusion measures the degree of change in the output as a result of slight change in the input. Most of the tests which a block cipher is subjected to treats the entire block of data as a single unit [6], and as a result, seldom reveals the bit level weaknesses.

The proposed scheme elicits relationship among the bits of the output vector. If the underlying block cipher does its encryption of the plain text in such a manner that a bit pair *(i,j)* are related, then knowing one bit discloses the other, thereby reducing the search space significantly. The scheme treats the underlying block cipher as a black box, and it determines the relationship on the basis of the input fed and the output generated by it.

I. TERMINOLOGY

A. *Bit-by-bit successful matches*

Consider two n bit binary strings, A and B. Then A_i is compared with B_i and if they are identical, then it is counted as a successful match, where A_i and B_i refers to the i^{th} and j^{th} bits of the string A and B, respectively.

B. *Relationship Test (R-Test)*

The idea is to exploit relationship among the bits of the presumably random n bit sequence. The objective of the test is not, in any way, to reveal the relationship, but to examine whether any relationship exist.

The scheme uses a randomly selected n-bit block of plain text (say P), which is then encrypted using the underlying cipher to produce the corresponding cipher block (say C). A matrix of size $n \times n$ is produced (say P_i), where each row of the matrix is a new plain text block in itself derived from the original block by flipping the bit at the i^{th} position, i.e. $P_i[i][j]=P[j]$ (+) e_i , where e_i is a zero vector containing *1* at the i^{th} position

$$P_i = \begin{pmatrix} p[0,0] & \cdots & p[0,n-1] \\ \vdots & \ddots & ,\vdots \\ p[n-1,0] & \cdots & p[n-1,n-1] \end{pmatrix}$$

Next, each row of the P_i matrix is fed as input to the underlying cipher to produce the corresponding cipher text, which is stored as the i^{th} row of the C_i matrix of size $n \times n$.

$$C_i = \begin{pmatrix} c[0,0] & \cdots & c[0,n-1] \\ \vdots & \ddots & \vdots \\ c[n-1,0] & \cdots & c[n-1,n-1] \end{pmatrix}$$

At this point, the scheme kicks in to produce another matrix (say *X*) of size *nxn*, where i^{th} row of the matrix is obtained by bitwise addition (modulo 2 addition) of the C_i vector with the *C* vector [4], i.e. $X[i]=C_i[i]$ (+) $C[i]$ [2].

$$X=\begin{pmatrix} x[0,0] & \cdots & x[0,n-1] \\ \vdots & \ddots & \vdots \\ x[n-1,0] & \cdots & x[n-1,n-1] \end{pmatrix}$$

The scheme then compares the i^{th} column of the *X* matrix with each of the other columns, where *0<=i<=(n-1)*. The algorithm of the proposed scheme is given below:

For each pair of bits (imp)

Compare the i^{th} column and the j^{th} column

(This might reveal a relationship between the i^{th} and j^{th} bits)

Worst case:

- The columns are identical, or
- No match is found.

Ideal case:

- n/2 successful matches found.

II. ALGORITHM

Input-Matrix *A* of size *nxn* (obtained in the same way as the *X* discussed in the previous section)
Output- An upper triangular matrix *B*
Method-

```
For i=0 to (n-1)
{       For j=i+1 to (n-1)
        {       B[i][j]←0
                For k=0 to (n-1)
                {       If A[k][i]=A[k][j]
                                B[i][j]←B[i][j] +1
                }
        }
}
```

Note- there are *(n-1) + (n-2) + …+1 = n(n-1)/2* entries in the upper triangular matrix and each of these entries ideally should have the value *n/2*, i.e. the i^{th} and the j^{th} column has *n/2* bit-by-bit successful matches. However, if an entry deviates significantly from the ideal value, then the i^{th} and the j^{th} bits are related in some sense. And if significant number of entries deviate from the ideal value, then it can be concluded that the underlying cipher has an inherent weakness.

A. *Proof of correctness*

Ideally each bit should change with a probability of *0.5*. That is,

$P(i^{th}$ *bit changes*$)=P(j^{th}$ *bit changes*$)=0.5$,

where *i* and *j* are any arbitrary bits. If the changes in the i^{th} and the j^{th} bit are random, then

$P(j^{th}$ *bit changes* $|$ i^{th} *bit has changed*$)=P(j^{th}$ *bit does not changes* $|$ i^{th} *bit has changed*$)=0.5$.

Now, since

$P(j^{th}$ *bit changes* $|$ i^{th} *bit has changed*$)=P(j^{th}$ *bit changes*$)$

it implies that j^{th} and i^{th} bits are not correlated, which implies that

$P(i^{th}$ *bit changing AND* j^{th} *bit changing)=P(*i^{th} *bit changing) .P(*j^{th} *bit changing)*

Or,

$P(i^{th}$ *bit changing AND* j^{th} *bit changing)=(0.5)*(0.5)=0.25*

and

$P(i^{th}$ *bit NOT changing AND* j^{th} *bit NOT changing)=P(*i^{th} *bit NOT changing) .P(*j^{th} *bit NOT changing)*

Or,

$P(i^{th}$ *bit NOT changing AND* j^{th} *bit NOT changing)=(0.5)*(0.5)=0.25*

Now,

P (i^{th} *bit changes AND* j^{th} *bit changes)* OR *(*i^{th} *bit NOT changes AND* j^{th} *bit NOT changes)* will be given by

$P(i^{th}$ *bit changes AND* j^{th} *bit changes) +* $P(i^{th}$ *bit NOT changes AND* j^{th} *bit NOT changes)*

=0.25 +0.25

=0.5

=> if we are considering *n* observations, probability of changing of each bit will become *0.5*n* or n/2.

B. Analysis

The scheme is analyzed using the TEST CIPHER described in [1]**.**

- **Objective**

The objective is to determine the secret key as is the case with other cryptanalysis techniques.

- **Assumptions**

It is assumed that the plain text block is known, the corresponding cipher text block is also known and the result of the Bit Relationship Test is available.

- **Effect of BRT**

Using exhaustive key search, the correct key can be determined in 2^8 guesses (in worst case). The sub- goal is to reduce the possible key space. Now, let us assume that the results of BRT reveal the fact that the i^{th} and the j^{th} bits of the cipher text are related in some sense. By relationship between bits, it is meant that either if the i^{th} bit of the cipher test is *0/1* then the j^{th} bit is also *0/1*, or if the i^{th} bit is *0/1* then the j^{th} bit is *1/0* with a very high degree of probability.

If the observed i^{th} bit and j^{th} bit of the cipher text are different, whereas the result of the BRT shows that most of the time they are similar, then it can be concluded that the disparity is because of the key bits which acted on the bit corresponding to the i^{th} and j^{th} bits in the plain text, which further implies that the referred key bit should be complementary. And even if there is parity between the observed cipher text bits and the result of the BRT, it implies that the key bits have same effect on both the bits, which further implies that both the referred key bits are identical with a very high degree of probability. Moreover, if the result of BRT shows that the concerned i^{th} and j^{th} bit are complementary most of the time and the observed cipher text shows otherwise, then this is again due to the key bit acting upon them, which implies that the concerned key bits are complementary too. Whereas, if the expected and the observed bits are identical, this would imply that the concerned bits are identical.

C. Experimental Results of BRT

Two popular Block Ciphers have been subjected to BRT namely Data Encryption Standard (DES) and Advanced Encryption Standard (AES) [5]. The results obtained are listed in Table 1.

Table 1: Results of BRT on AES and DES

Block Ciphers	**# Entries having deviation(δ)**			
	δ =0%	**δ =6.25%**	**δ =12.5%**	**δ >12.5%**
DES	9.05%	65.87%	21.95%	3.13%
AES	6.75%	74.04%	18.87%	0.34%

Note that the deviation is computed on the basis of the ideal situation, which is 32 in case of DES and 64 in case of AES. It should also be noted that the percentage of entries in a particular column is computed on the basis of the total number of entries, which is 2016 in case of DES and 8128 in case of AES.
The results obtained are represented graphically in fig. 1 and fig. 2.

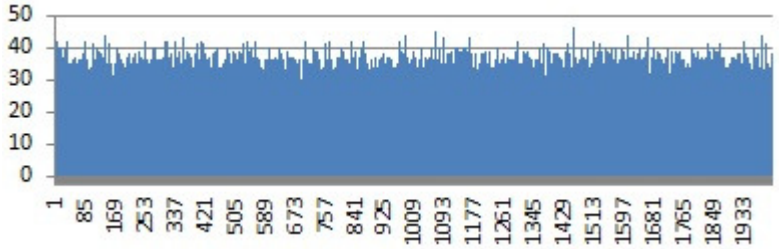

Fig. 1: Graphical representation of the BRT results on DES.

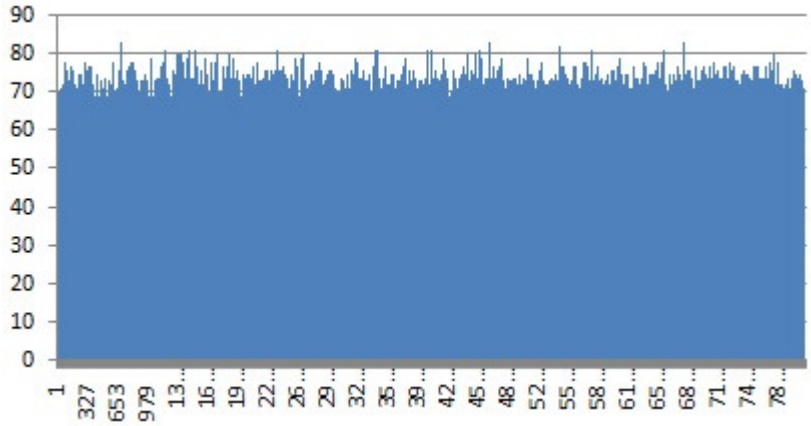

Fig. 2: Graphical representation of the BRT results on DES.

After obtaining the results, they are analyzed statistically by obtaining the mean, standard deviation and coefficient of variance. The coefficient of variance gives the degree of variation in the observation, the larger the coefficient of variance the higher the degree of variation. The Table 2 summarizes the results.

Table 2: Summary statistics of BRT on AES and DES

Statistic	**DES**	**AES**
Mean	32.52529762	64.05967
Standard Deviation	3.926540716	5.62726
Coefficient of variance	12.07226683	8.784404

III. CONCLUSION

Generally, it can be stated that if two bits of a block or different block are related in some sense, then the relationship can be explored to correctly guess the key bit which operate on those bits to a large extent and, as a result, causes a reduction in the actual key space. Moreover, the better the diffusion characteristic of the underlying cipher, the lesser the chances of such an attack.

From the results obtained, it can be concluded that the results obtained from BRT on DES shows higher degree of variation as compared to the results obtained in case of AES. Ideally, mean in case of DES should have been 32 and in case of AES it should have been 64. The observed results are not too far from the ideal situation, although it can be stated that the mean in case of AES is much more close to the ideal case as compared to DES. From the analysis, it can be concluded that AES has better diffusion characteristic as compared to DES.

REFERENCES

[1] Bhowmik, D., Datta, A., & Sinha, S.,2014," A Bit-level Block Cipher Diffusion Analysis Test – BLDAT", Proc. of the 3rd International Conference on Frontiers in Intelligent Computing Theory & Application (FICTA), *AISC* 327 Vol. 1 *Springer* ,667-674.

[2] Castro, J.C.H., Sieria, J.M., Seznec, A., Izquierdo, A., Ribagorda, A., 2005. "The Strict Avalanche Criterion Randomness Test", Mathematics and Computers in Simulation 02/2005, Elsevier Publication, 68(2005), 1-7.

[3] Deniz Toz, Ali Doğanaksoy, Meltem Sönmez Turun, "Statistical Analysis of Block Ciphers", Ulusal Kriptologi Sempozyumu, Ankara, Turkey (2005), 56-66.

[4] Katos,V, 2005. "A Randomness Test for Block Ciphers", Applied Mathematics and Computation, Elsevier Publication, 162(2005), 29-35.

[5] Paar, C. and Pelzl, J., 2010. "Understanding Cryptography", Berlin: Springer-Verleg.

[6] Soto J., L. Bassham, "Randomness Testing of the Advanced Encryption Standard Finalist Candidates", Computer Security Division, National Institute of Standards and Technology, 2000.