ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

An Approach towards Analyzing Strict Key Avalanche Criterion of Block Ciphers

Dipanjan Bhowmik[1], Avijit Datta[2], Sharad Sinha[3]

Research Scholar, Department of Computer Science and Applications, University of North Bengal, W.B., India[1]

Assistant Professor, Department of Computer Science and Application, University of North Bengal, W.B., India[2]

ABSTRACT: A scheme pertaining to the analysis of Strict Key Avalanche Criterion possessed by a block cipher has been proposed here. A block cipher is said to have strong Strict Avalanche Criterion if a small change in the key causes massive and random changes in the corresponding ciphertext. The paper also highlights the importance of Strict Key Avalanche Criterion (SKAC) with respect to the attacks that a block cipher may be subjected to. Apart from the scheme, the paper also analyzes the results obtained from the test when two of the well known and well documented cipher; namely Data Encryption Standard (DES) and Advanced Encryption Standard (AES), were tested using it..

KEYWORDS: Strict Key Avalanche Criterion (SKAC), Strict Avalanche Criterion (SAC), Block Cipher**.**

I. Introduction

According to C.Shannon [11], the cryptographic strength of a block cipher directly depends on two aspects- they are the confusion and the diffusion characteristics of the cipher. Apart from these two aspects, another important characteristic that a block cipher should posses is a sound key structure. A block cipher having strong confusion and diffusion characteristics but a poorly designed key structure may not be of any use as an attacker might as well attack the cipher and retrieve critical information about the key being used to encrypt the file. So, for a block cipher to be secure apart from having strong confusion and diffusion characteristic, it should also have a strong key structure so that no information can be retrieved about the plaintext being encrypted or the key used to encrypt it.

In this paper, a straight forward and an easy to implement version of a test aimed at analyzing the strength of the cipher with respect to its key structure has been presented. The test analyzes the the key structure using a method called the Strict Key Avalanche Criterion (SKAC)[7]. A block cipher is said to have a strong SKAC if a small change in the key causes massive and random changes in the resulting ciphertext. In that sense, it is similar to the Strict Plaintext Avalanche Criterion (SPAC), but instead of applying the Strict Avalanche Criterion (SAC) on plaintext in SKAC it is applied on the key.

A block cipher having poor SPAC is prone to chosen plaintext attack [3], wherein the attacker has the ability to choose plaintext P_i and to view their corresponding ciphertexts C_i. On the other hand, if a block cipher has poor SKAC, then it is prone to Known plaintext attack [3], where in the attacker has access to pairs (P_i,C_i) for $i = 1,2,\dots n$ of known plaintext and their corresponding ciphertexts. This attack is considered to be highly practical especially when it is compared to the chosen plaintext attack which is very difficult to implement. Moreover, if a cipher is vulnerable to known plaintext attack, it is automatically vulnerable to chosen plaintext attack as well, but not necessarily the opposite. Techniques such as “public word method” which is used for solving simple transposition or classical substitution ciphers are nothing but simplified version of the known plaintext attack. In modern cryptology, linear cryptanalysis [10] is an example of known plaintext attack where as much fancier differential cryptanalysis [2] is an example of chosen plaintext attack. In fact, differential cryptanalysis is a rare technique for which conversion from chosen plaintext attack to known plaintext attack is possible. From the above discussion, it is clear that a block cipher should have strong SKAC properties. In fact, a block cipher should have SKAC property at least as strong as it has SPAC, if not more.

The test scheme proposed in the paper is simple to understand and easy to implement as it uses the Bit Level Diffusion Analysis Test (BLDAT) [1] with some modifications. Originally BLDAT was designed to analyze the diffusion characteristic of the underlying block cipher with respect to the plaintext avalanche criterion whereas the proposed test uses it to analyze the key avalanche criterion. Moreover, as BLDAT, the proposed test also treats the underlying cipher as a black box, and as a result, the test can be applied to whole host of block ciphers without bothering about their internal structures.

II. Related work

Over time, many testing strategies have been developed in order to test the cryptographic strength of underlying Block Ciphers, and one of the most important is the SAC.

The avalanche criterion was originally proposed for s-boxes by Webster and Tavares in 1986[13], which was further generalized to the strict avalanche criterion by Forre in 1990[8]. The SAC test is aimed at analyzing the diffusion characteristics of the underlying cipher. A cipher is said to have very good diffusion properties if a slight change in the input causes huge changes in the output. Mathematically SAC can be explained as:

$$\forall x, y \mid H(x,y) = 1, average\left(H\left(F(x), F(y)\right)\right) = \frac{n}{2}$$

Where x,y, are two binary strings of length n and H() denotes the *Hamming Distance* between the two strings. Thus, the function to have an avalanche effect, the Hamming Distance between the output of a random input vector and one generated by randomly flipping one of its bits should be on an average$\frac{n}{2}$. That is, a minimum input change (1 bit) is amplified and produces a maximum out put change (half of the bits) on an average.

The SAC test proposed in the paper titled "The strict avalanche criterion randomness test" [4] implies a more stringent constraint which is mathematically described as:

$$\forall x, y \mid H(x,y) = 1, \left(H\left(F(x), F(y)\right)\right) \approx B\left(\frac{1}{2}, n\right)$$

That is, the hamming distance between the output generated by *F()* using a random *n*-bit string and a string obtained by flipping one bit at a random position should approximate *Binomial Distribution* with parameters $\frac{1}{2}$ and *n*, this implies the avalanche effect as mean of Binomial distribution to be $\frac{n}{2}$.

The tests included in [12] are versions of SAC. It includes *test to evaluate different key values, distinguishing properties test* and *padding tests*.

In this version of the SAC test, a matrix of dimension n x n is produced where n is the block size which is obtained by decimally summing over m matrices, each of which is equivalent to the φ matrix defined in [9]. Each of the entries of the newly formed matrix is defined by m which is the number of randomly chosen plaintext used to generate the corresponding φ matrix. If all the entries end up having 0.5, then the underlying cipher is said to have good diffusion properties otherwise not.

The strict key avalanche criterion (SKAC) test described in [7] is a test to measure the diffusion characteristics of a cipher, generates a matrix of dimension $n \times m$, where *n* is the length of the plaintext/ cipher text block and *m* is the length of the key , where in all of its entries are initialized to zero. The test as described in the paper begins by randomly picking a plain text *p* and *r* keys k_i for$i = 1,2, \ldots r$. Then for each of these *r* keys, new keys are generated by flipping the j^{th} bit of each key i.e.k_{ij} for $j = 1,2, \ldots m$.

Next, for each of the newly generated keys K_{ij} derived from the key K_i by flipping the j^{th} bit, an avalanche vector $U_{ij} = E(k,p) \oplus E(k_{ij},p)$ is produced. This process is carried out for each of the derived keys generated from the randomly picked keys. Then, each of the U_{ij} vectors are added decimally for i=1,2,…r and *j=1,2,…m* in the $n \times m$ matrix. Next, each of the entries of the n x m matrix is divided by *r* and the resultant matrix thus obtained is referred to as the *Avalanche Matrix*. The null hypothesis used in this case is that the expected value of each of the *nm* entries is$\frac{1}{2}$. Next, a standard normal variable $Z_{ij}=2\sqrt{r}(b_{ij}-0.5)$ is calculated for *i=1,2,…n* and *j=1,2,…m.* In order to obtain more accurate SKAC characteristic of the underlying block cipher, the test is conducted for *t* randomly chosen plain text blocks & Fisher Pierson method is applied. Moreover, Kolmogrov-Snimov test statistic is applied to determine whether nm independent probabilities satisfy uniform distribution in [0,1].

III. Proposed Scheme

The algorithm takes as input a random m-bit plaintext block P(for DES [4] m=64 and for AES [5] m=128) and a random n-bit key K(for DES n=56 and for AES n=128).The algorithm then generates the corresponding ciphertext $C = E(P,K)$ (for DES the ciphertext in 64 bits and for AES the ciphertext is 128 bits). Next, using the original key K, a bunch of keys K_i are generated where $i = 0,1, \dots (n-1)$such that each key K_i differ from the original key K at the i^{th} position. Using each of the n generated keys, the same original plaintext block is encrypted to generate C_i's where each $C_i = E(P, K_i)$ for $i = 0,1, \dots (n-1)$. Each of these C_i's are then bitwise XORed with the original ciphertext C and stored as the i^{th} vector of the SKAC matrix of order $n \times m$. Then the number of 1's in each column of the SKAC matrix is counted and stored at j^{th} position of the V vector where $j = 0,1,2, \dots (m-1)$.

Ideally, each of the m entries in the V vector should be $\frac{n}{2}$ (for DES $\frac{n}{2} = 28$ & for AES $\frac{n}{2} = 64$) and greater the deviation from the ideal value, the more the corresponding bit is vulnerable to attacks that exploit this weakness..

A. Algorithm

```
Step 1: Select a random plaintext block $P$ of $m$-bits.
Step 2: Select a random key $K$ of $n$-bits.
Step3: Generate the corresponding ciphertext $C = E(P, K)$.
Step 4: For each of the $n$-bit key $K$, repeat
        Step 4.1: Generate a key $K_i = K \oplus e_i$, where ei is a zero vector with a 1 at the $i^{th}$ position.
        Step 4.2: Generate$C_i = E(P, K_i)$.
        Step 4.3: Generate $SKAC_i = C \oplus C_i$, where SKAC is a matrix of order $n \times m$.
Step 5: For each of the $m$ columns of the SKAC matrix $V_j = number\ of\ 1's\ \text{in the}\ j^{th}\ column$.
```

IV. Experimental Results

Two of the most widely documented block ciphers, namely DES and AES were put to test. The results obtained are presented in sections III(A) and III(B).

A. *Experimental Results for DES:*

The proposed scheme was used to test the SKAC of Data Encryption Standard (DES). A summary of the results obtained from the test are listed in Table 1.

Key	Expected Mean	Observed Mean	Std. Deviation	Variance	Coefficient of Variance
Sparse	28	27.90625	4.010774	16.08631	14.37232
Dense	28	28.5625	3.812573	14.53571	13.34818
Random	28	28.23438	3.878071	15.03943	13.73528

Table 1: Experimental results for DES.

Moreover the vector V corresponding to the inputs P = ”ABCDEFGH” and K=$(00110100111010110001110010010110110110111000000000110011)_2$ is presented in Table 2.

v[0]=27	v[8]=29	v[16]=26	v[24]=26	v[32]=27	v[40]=29	v[48]=29	v[56]=20
v[1]=29	v[9]=32	v[17]=26	v[25]=29	v[33]=26	v[41]=32	v[49]=38	v[57]=27
v[2]=31	v[10]=24	v[18]=25	v[26]=24	v[34]=36	v[42]=27	v[50]=25	v[58]=22
v[3]=32	v[11]=29	v[19]=31	v[27]=28	v[35]=23	v[43]=22	v[51]=31	v[59]=30
v[4]=31	v[12]=29	v[20]=31	v[28]=23	v[36]=35	v[44]=22	v[52]=31	v[60]=23
v[5]=26	v[13]=28	v[21]=27	v[29]=32	v[37]=29	v[45]=27	v[53]=31	v[61]=27
v[6]=31	v[14]=32	v[22]=31	v[30]=39	v[38]=25	v[46]=26	v[54]=32	v[62]=25
v[7]=27	v[15]=27	v[23]=27	v[31]=35	v[39]=27	v[47]=24	v[55]=25	v[63]=30

Table 2: The V vector corresponding to P=”ABCDEFGH” and K=$(00110100111010110001110010010110110110111000000000110011)_2$

DOI: 10.15680/IJIRCCE.2016. 0406258

B. *Experimental results for AES:*

A summary of the results obtained when the Advanced Encryption Standard (AES) was tested using the proposed scheme are presented in Table 3.

Key	Expected Mean	Observed Mean	Std. Deviation	Variance	Coefficient of Variance
Sparse	64	64.578125	5.704825109	32.54502953	8.833990007
Dense	64	64.601563	5.9411018	35.29669	9.1965296
Random	64	64.13281	5.823346	33.91136	9.080135

Table3: Experimental results for AES.

The complete *V* vector corresponding to *P* =”ABCDEFGHIJKLMNOP” and *K*=(54 199 205 26 35 133 133 245 67 48 109 53 187 186 221 34)$_{256}$ is provided in Table 4.

V[0]=58	V[16]=64	V[32]=77	V[48]=65	V[64]=62	V[80]=76	V[96]=59	V[112]=67
V[1]=68	V[17]=68	V[33]=69	V[49]=56	V[65]=67	V[81]=63	V[97]=66	V[113]=53
V[2]=60	V[18]=67	V[34]=55	V[50]=58	V[66]=76	V[82]=60	V[98]=61	V[114]=69
V[3]=54	V[19]=69	V[35]=66	V[51]=63	V[67]=64	V[83]=64	V[99]=62	V[115]=73
V[4]=68	V[20]=67	V[36]=74	V[52]=68	V[68]=63	V[84]=66	V[100]=62	V[116]=58
V[5]=60	V[21]=66	V[37]=61	V[53]=68	V[69]=71	V[85]=75	V[101]=63	V[117]=64
V[6]=67	V[22]=56	V[38]=59	V[54]=65	V[70]=67	V[86]=71	V[102]=64	V[118]=65
V[7]=50	V[23]=62	V[39]=68	V[55]=64	V[71]=72	V[87]=55	V[103]=59	V[119]=68
V[8]=66	V[24]=70	V[40]=67	V[56]=65	V[72]=64	V[88]=62	V[104]=63	V[120]=61
V[9]=52	V[25]=80	V[41]=70	V[57]=63	V[73]=63	V[89]=57	V[105]=67	V[121]=59
V[10]=71	V[26]=66	V[42]=71	V[58]=63	V[74]=58	V[90]=65	V[106]=56	V[122]=62
V[11]=68	V[27]=71	V[43]=69	V[59]=56	V[75]=74	V[91]=64	V[107]=54	V[123]=77
V[12]=53	V[28]=60	V[44]=70	V[60]=63	V[76]=64	V[92]=62	V[108]=70	V[124]=60
V[13]=63	V[29]=59	V[45]=63	V[61]=64	V[77]=59	V[93]=65	V[109]=63	V[125]=65
V[14]=64	V[30]=64	V[46]=62	V[62]=63	V[78]=64	V[94]=59	V[110]=63	V[126]=60
V[15]=62	V[31]=70	V[47]=48	V[63]=75	V[79]=61	V[95]=69	V[111]=66	V[127]=57

Table 4: The *V* vector corresponding to *P*=”ABCDEFGHIJKLMNOP” and K=(54 199 205 26 35 133 133 245 67 48 109 53 187 186 221 34)$_{256}$.

V. DISCUSSION

The results obtained in both the cases are compared using Coefficient of Variance. Coefficient of variance measures the amount of deviation of data points about the mean. It is calculated as follows

$$Coefficient\ of\ Variance = \frac{Standard\ Deviation}{Mean}$$

As Coefficient of Variance is defined as the ratio of Standard Deviation with respect to the mean, it provides a way to compare the variations in different data sets even if the means are drastically different.

Table 5, gives an account of the Coefficient of Variances for both DES and AES with respect to different types of keys.

Key	Coefficient of Variance	
	DES	AES
Sparse	14.37232	8.833990007
Dense	13.34818	9.1965296
Random	13.73528	9.080135

Table 5: Comparison of Coefficient of Variance for DES and AES

From the results presented in table 5, it is clear that AES gives better results as compared to DES with respect to the Key Avalanche Criterion.

VI. CONCLUSION

As discussed in section 1, along with confusion and diffusion characteristics of the cipher, the key structure also plays an important role in making the cipher cryptographically secure. In such a situation, the proposed scheme may serve as a tool to analyze the key structure and hence the strength of the underlying block cipher.

REFERENCES

1. Bhowmik, D., Datta, A., & Sinha, S.,“ 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 ,pp.667-674,2014.
2. Biham, E., & Shamir, A.,“Differential Cryptanalysis of DES like Cryptosystems”, Journal of Cryptology, vol. 4,pp.3-72,1991.
3. Biryukov, A “Encyclopedia of Cryptography and Security” Springer.
4. Castro,J.C.H.,Sieria,J.M.,Seznec,A.,Izquierdo,A.,Ribagorda,A.,“The Strict Avalanche Criterion Randomness Test”, Mathematics & Computers in Simulation, Elsevier Publication,68,pp.1-7,2005.
5. Coppersmith, D., “The Data Encryption Standard and its Strength Against Attacks”, IBM Journal of Research and Development, 38(3) 243,1994.
6. Daemen, J, and Rijmen, V., “AES Proposal: Rijndael”. National Institute of Standards and Technology. pp. 1,2003.
7. Dawson, E., Gustafson, H.,& Petritt, A.N.,“Strict Key Avalanche Criterion”,1992.
8. Forre, R.,“The strict avalanche criterion special properties of Boolean functions and an extended definition”, Advances in Cryptography-CRYPTO’ 88, Springen-Verlag,pp.450-468,1990
9. Katos,V.,“A randomness test for block ciphers”. Applied Mathematics & Computation ,Elsevier Publications,162,pp.29-35,2005.
10. Matsui, M., and Yamagishi, A., “A new method for known plaintext attack of FEAL cipher”. Advances in Cryptology – EUROCRYPT,1992
11. Shannon, C.,“Communication Theory of Security Systems”,Bell Systems Technical Journal, vol-28,1949.
12. Toz, D., Doganaksoy,A., A& Turan, M.S., “Statistical Analysis of Block Ciphers”.
13. Webster, A.F., & Taveres,S.F.,“On the design of s-boxes”, Advances in Cryptography-CRYPTO’85,Springer-Verlag,pp.523-534,1986.

BIOGRAPHY

Dipanjan Bhowmik is an UGC-JRF in the Department of Computer Science and Application, University of North Bengal. He received Master of Computer Application (MCA) degree in 2011 from University of North Bengal, WB, India. His research interest is Cryptology.

Avijit Datta is a Research Scholar in the Department of Computer Science and Application, University of North Bengal and Assistant Professor of Siliguri Institute of Technology, Siliguri. He received Master of Computer Application (MCA) degree in 2005 from UPTU, UP, India. His research interest is Cryptology.

Sharad Sinha is an Assistant Professor of University of North Bengal. He received Ph.D. degree in 2008 and Master of Computer Application (MCA) degree in 1992 from University of North Bengal, WB, India. His research interest is Cryptology.

DOI: 10.15680/IJIRCCE.2016. 0406258