COMPARISON OF THE BLOCK CIPHERS DES AND IDEA

Melek D.Yücel* , R.Cüneyt Acar**
*EE.Dept.of METU and TÜBİTAK-BİLTEN
**ASELSAN Inc. MST Division

Abstract-We propose a new measure, the Avalanche Weight Distribution (AWD) as a rough but quick test criterion for block ciphers. We evaluate the AWD curves of DES and IDEA. We observe that while the 2nd and higher rounds of IDEA give perfect AWD curves, such perfect curves are hardly observed even at the higher rounds of DES. We also examine the effects of modifying and removing the MA-Box of the IDEA algorithm.

1. INTRODUCTION

DES, an acronym for the Data Encryption Standard, is the name of the Federal Information Processing Standard (FIPS), which describes the data encryption algorithm (DEA) [1]. DEA, often called DES, has been originally developed by IBM, the National Security Agency (NSA). The National Bureau of Standards (NBS) has also played a substantial role in the final stages of development. DES has been extensively studied since its publication and is the best known and widely used symmetric algorithm in the world.

DES is a symmetric block cipher, specifically a 16-round Feistel cipher [2]. DES has a 64-bit block size and uses a 56-bit key during execution (8 of the bits are the parity bits out of 64-bit user secret key).

The block cipher IDEA (International Data Encryption Algorithm) has been proposed by X.Lai and J.L.Massey [3]. Its previous version is called PES (Proposed Encryption Standard). In PES and IDEA, the plaintext and the ciphertext are 64-bit blocks, while the secret key is 128 bits long. Both ciphers are based on the new design concept of "mixing operations from different algebraic groups". The required "confusion" is achieved by successively using three "incompatible" group operations on pairs of 16-bit subblocks. The IDEA cipher is an improved version of PES and has been developed to increase the security against differential cryptanalysis.

The diffusion property of IDEA is provided by the multiplication-addition structure (MA-Box) which transforms two 16 bit subblocks (I_1 and I_2) into two 16 bit segments (O_1 and O_2) controlled by two 16-bit subkeys (Key1, Key2). The structure of the MA-Box is given in Fig.1.

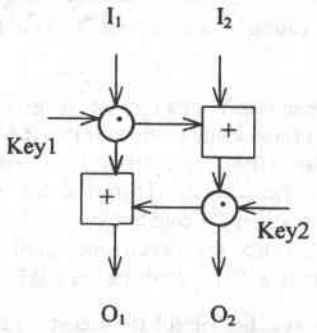

Figure 1. MA-Box of IDEA

2. BACKGROUND

It will be useful to explain the notation that will be used. The ciphertext of the algorithm is $C=(c_n,\ldots,c_2,c_1)$, the plaintext of the algorithm is $P=(p_n,\ldots,p_2,p_1)$, the plaintext difference is $\delta=(\delta_n,\ldots,\delta_2,\delta_1)$. Owing to a plaintext change δ, the ciphertext change is C^δ. The ciphertext change C^δ will be called the avalanche vector and the Hamming weight of C^δ will be represented as $w(C^\delta)$. A specific plaintext difference, whose Hamming weight is 1, is called e_i, and defined as a vector whose i'th bit is 1 and others are 0.

Definition: The Avalanche Weight Distribution (AWD) is defined as the histogram of $w(C^\delta)$ versus $w(C^\delta)$.

In order to evaluate AWD curves, we use a subprogram which does the following:

- The plaintext P_1 is selected randomly, and the corresponding ciphertext C_1 is obtained at a specific round of the encryption algorithm.
- The plaintext

$$P_2=P_1 \oplus e_i \qquad (1)$$

where $\oplus$ is a bitwise EXOR operator, is found for a fixed value of plaintext difference $\delta=e_i$. After the same

specified round of encryption, the second ciphertext C_2 is obtained.

- The ciphertext difference corresponding to the plaintext difference $\delta=e_i$,

$$C^{\delta}=C_1 \oplus C_2 \qquad (2)$$

is obtained. Hamming weight of C^{δ}, $w(C^{\delta})$, is calculated. To store the occurrence number of $w(C^{\delta})$, we use a counter for each $w(C^{\delta})$ value in the range (0,n).

The mentioned subprogram is executed 10000 times for a fixed value of the user key (64-bit for DES, 128-bit for IDEA), and fixed $\delta=e_i$, but for 10000 different plaintexts P_1. Therefore the sum of the numbers in all $w(C^{\delta})$ counters ($0 \le w(C^{\delta}) \le n$) is 10000. Then we sketch the occurrence number of $w(C^{\delta})$ values versus $w(C^{\delta})$ to evaluate the AWD curve.

It will also be helpful to discuss what we expect from the AWD of an ideal algorithm which satisfies the diffusion property mentioned by Shannon [4]. The probability of finding any particular number of ciphertext bit changes, $w(C^{\delta})$, in a ciphertext of n bits is:

$$\Pr\left(w(C^{\delta})\right)=\frac{\binom{n}{w(C^{\delta})}}{2^n} \qquad (3)$$

which is the binomial expression.

In order to give an idea about what we should expect from AWD of an ideally diffused encryption algorithm, we sketch 10000 x $\Pr(w(C^{\delta}))$, for n=64 in Fig.2. The ideal distribution is symmetrical with an average value of 32 bits.

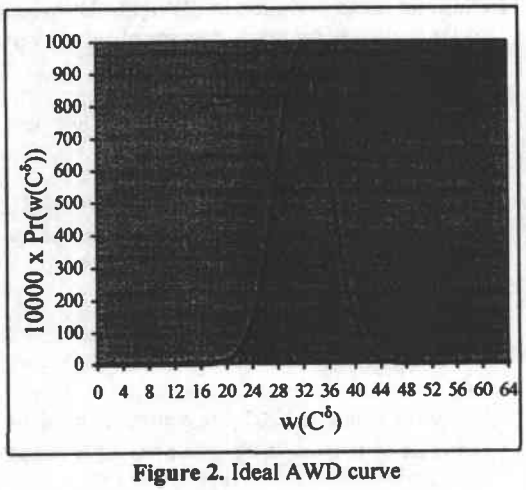

Figure 2. Ideal AWD curve

3. AWD CURVES OF DES AND IDEA

We sketch the AWD curves of DES and IDEA at specific rounds of those algorithms. Horizontal axis shows all possible $w(C^{\delta})$ values in the range (0,64). In the sketches, we use "Algorithm #R" to indicate the AWD at the #'th round of the algorithm. For instance: "DES 1R" shows the AWD at the 1'st round of DES.

Through our investigations, we have observed that for the DES algorithm, all $\delta=e_i$'s have similar AWD curves, therefore $w(C^{\delta})$ histograms for $\delta=e_{35}$ are sketched as representative.

In Fig.3, AWD curves of 1-round and 2-round versions of DES are given. We observe that if a single bit (35. bit) of the plaintext is changed, first round of DES changes less than 9 bits of the ciphertext, whereas at the end of the 2'nd round an average of 20 ciphertext bits are changed.

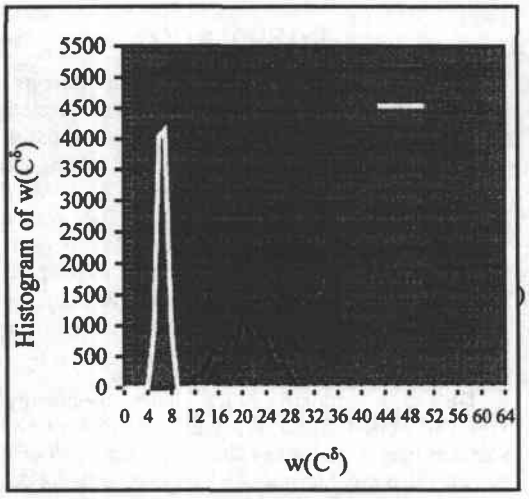

Figure 3. AWD curve of DES, $\delta=e_{35}$, 1,2-round version

In Fig.4, AWD curves of 3-round and 4-round versions of DES are depicted for the same $\delta=e_{35}$. As it is seen from the figure, as the encryption round number is increased, the diffusion in the ciphertext is also increased; and the AWD becomes more similar to the ideal curve given in Fig.2. Although both curves of Fig.4 are concentrated around the average value of 32 bits; yet the AWD for DES 4R is much closer to the ideal curve, and this behaviour is observed at higher rounds of DES as well.

In order to compare with DES, the AWD curves are also sketched for IDEA. It is observed that IDEA has an ideal-like AWD curve for some $\delta=e_i$'s even after one-round of encryption. In Fig.5, the AWD curve is sketched for i=34 and those values of i which give very similar AWD's are indicated in Table 1.

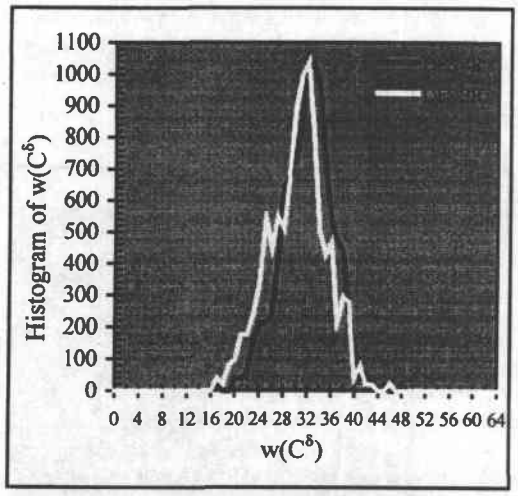

Figure 4. AWD curve of DES, $\delta=e_{35}$, 3,4-round version

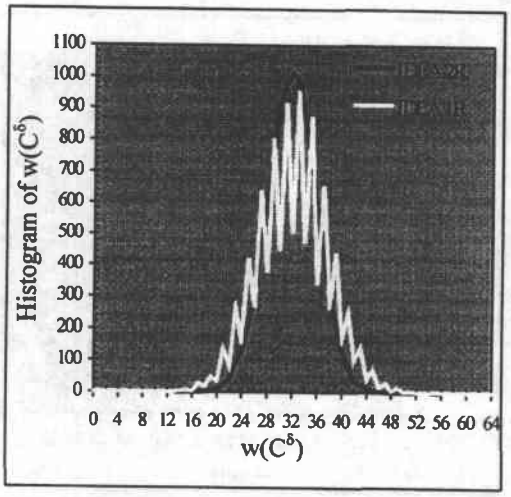

Figure 6. AWD curve of IDEA, $\delta=e_{41}$, 1,2-round version

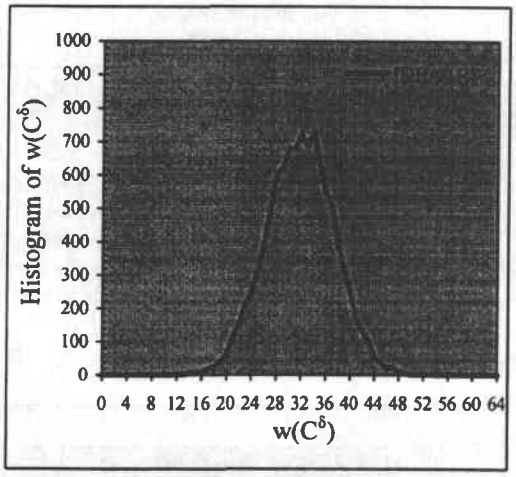

Figure 5. AWD curve of IDEA, $\delta=e_{34}$, at the 1st round

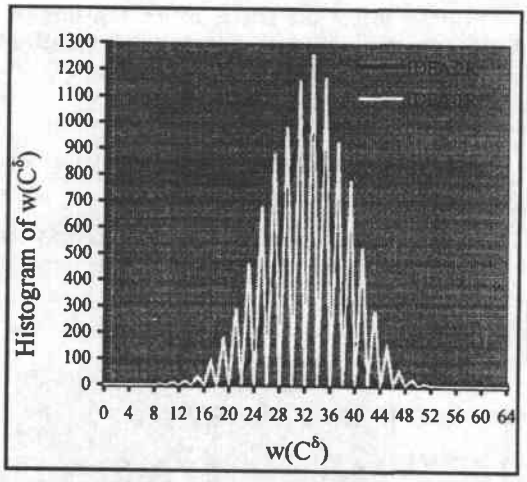

Figure 7. AWD curve of IDEA, $\delta=e_{17}$, 1,2-round version

For other values of δ, the AWD is oscillatory at the first round, however this behaviour is corrected at the second round. Oscillations are such that maxima occur at odd values and minima occur at even values of $w(C^{\delta})$. In Fig.6, the AWD curves are sketched for i=41, and those values of i which give very similar AWD's are indicated in Table 1.

The third type of AWD curves are observed for other values of δ, which are also oscillatory at the first round; however, all minima corresponding to even values of $w(C^{\delta})$ are exactly 0. This behaviour is also corrected at the 2nd round, as can be seen from Fig.7 sketched for i=17. Those values of i which give very similar AWD's are shown in Table 1.

For all values of the plaintext difference $\delta=e_i$, the 2nd and higher rounds of IDEA give perfect AWD curves. However, in the case of DES, such a perfect like behaviour is hardly observed even at the 10'th round as seen from Fig.8.

Table 1. Behaviour of IDEA for different e_i's

Location of the plaintext bit change, i	Behaviour
1-16,18,34,49-64	Similar to Fig.5
19-32,35-48	Similar to Fig.6
17,33	Similar to Fig.7

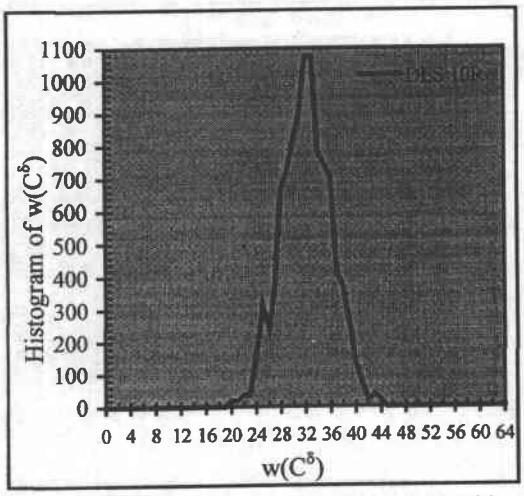

Figure 8. AWD curve of DES, $\delta=e_{35}$, at the10'th round

In order to see the effects of the MA-Box (see Fig.1) on the diffusion properties of the IDEA algorithm, we evaluate the AWD curves by:

1. removing the MA-Box
2. replacing one multiplier of the MA-Box with an adder.

In both cases, the value of $\delta=e_i$ which gives the worst AWD curve is found.

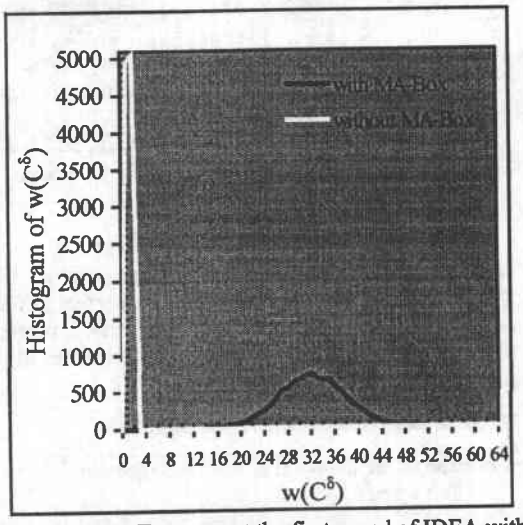

Figure 9. AWD curves at the first round of IDEA with and without MA-Box, for $\delta=e_{34}$

1. Removing the MA-Box: Fig.9 shows the effect of removing the MA-Box totally, at the first round. As the round number increases, this nonideal behaviour does not change much. Only a slight correction is observed for the behaviour of IDEA without MA-Box even at the last round as shown in Fig.10.

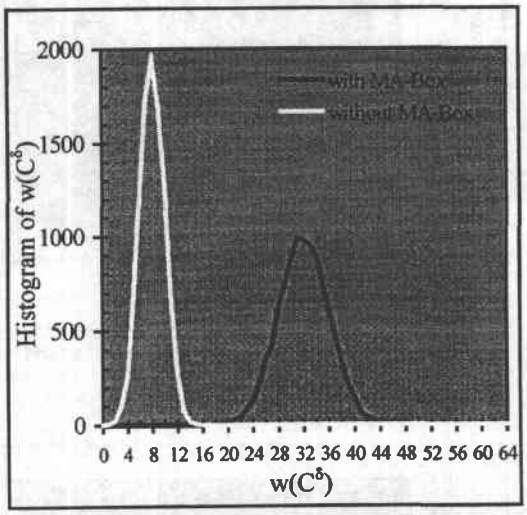

Figure 10. AWD curves at the last round of IDEA with and without MA-Box, for $\delta=e_{34}$

2. Modified MA-Box: Fig.11 shows the effect of making the modification mentioned above. The behaviour of modified IDEA that is seen in Fig.11 is corrected rapidly at the second round. The above mentioned AWD curve of IDEA with modified MA-Box at the second round is seen in Fig.12.

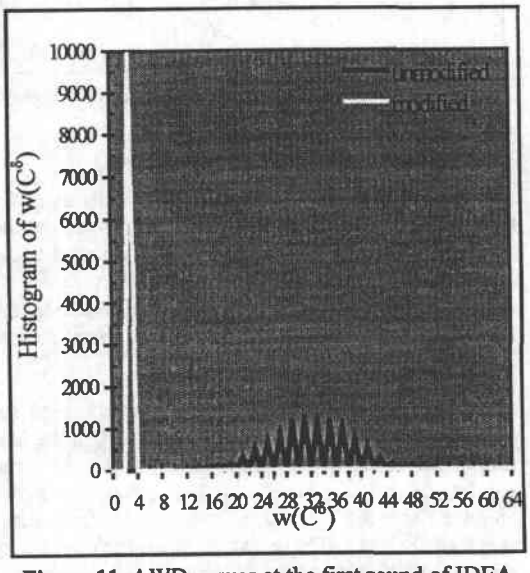

Figure 11. AWD curves at the first round of IDEA with unmodified and modified MA-Box, for $\delta=e_{17}$

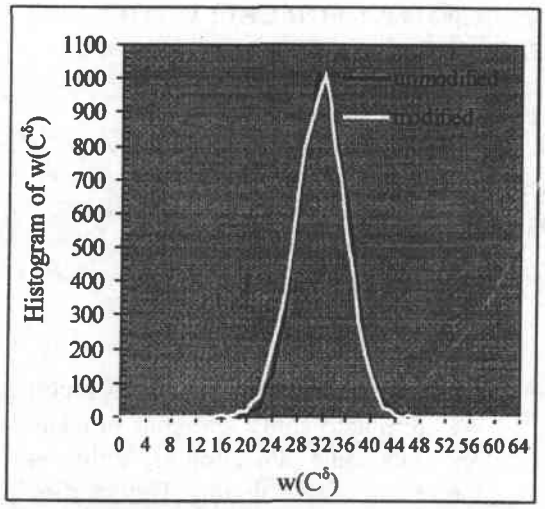

Figure 12. AWD curves at the second round of IDEA with unmodified and modified MA-Box, for $\delta=e_{17}$

4. CONCLUSION

We have seen that for all values of the plaintext difference $\delta=e_i$, the 2nd and higher rounds of IDEA give perfect AWD curves. However, in the case of DES, such a perfect like behaviour is hardly observed even at the 10'th round as seen from Fig.6.

In order to see how the presence of the MA-Box affects the AWD curves of the IDEA algorithm, we have first modified, then removed the MA-Box. We have observed that a modification in the form of replacing one multiplier with an adder distorts the AWD at the first round, but it can be corrected at the second round. However, if the MA-Box is removed completely, an ideal AWD curve is never obtained for any value of e_i, even at the last round of IDEA.

REFERENCES

[1] Data Encryption Standard, FIPS PUB 46 National Bureau of Standards, Washington, DC, 15 January 1977.

[2] H.Feistel, "Cryptography and Computer Privacy" Scientific American, v.228, n.5, May 1973, pp. 15-23.

[3] X.Lai, On the design and security of block ciphers, ETH Series in Information Processing, Volume 1, Editor: James L. Massey, Konstanz, Switzerland: Hartung-Gorre, 1992.

[4] C.E.Shannon."Communication theory of secrecy systems", Bell systems Technical Journal, vol.28, pp.656-715, 1949.