ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 6, June 2012

Design Implementation of IDEA to S-IDEA

Harivans Pratap Singh, Sweta Verma, Shailender Mishra

Abstract: - Large numbers of weak keys were found for IDEA (International Data Encryption Algorithm) [3, 4]. Also a new attack on round 6 of IDEA [5] has been detected. The paper proposes to increase the strength of the present algorithm to make it more secure. There are basically two propositions to increase the strength; firstly, by increasing the key size and secondly, by increasing the amount of diffusion in this paper, the key [5] size is increase from 128 bits to 256 bits. This increased key size will increase the complexity of the algorithm. To increase the amount of diffusion two MA blocks (multiplicative additive block) are used in a single round of IDEA as compared to one MA block used previously in a single round. With these modifications in the present algorithm one can increase the cryptographic strength of the algorithm. The 128 bit block is divided into eight 16- bit blocks on which functions of individual sub-keys is applied The proposed modified version of IDEA (known as Secure IDEA- "S-IDEA") can be seen as two sub-block of 64 bits running in parallel with each other. Each round consists of two further divisions i.e. Transformation followed by Sub-Encryption The algorithm still consists of 8 rounds plus 1 output transformation round; but now 12 sub-keys are used in each round - 8 in transformation round and 4 in sub-encryption round. The last round uses 8-keys. In total 104 sub-keys are used in 8+1 rounds. At the last round the eight 16- bit blocks are recombined to form a 128 bit cipher text block.

Keywords: **S-IDEA, Multiplicative Additive Block**

I. INTRODUCTION

Cryptography constitutes two words-"crypt"+"graphy" which means secret writing. It is a technique to code the data so that only people who share the secret key can decode the secret writing. An original message is known as the plaintext, while the coded message is called the cipher text. The process of converting from plaintext to cipher text is known as encryption; restoring the plaintext from the cipherext is called decryption. The many schemes used for encryption constitute the area of study known as cryptography. Cryptographic algorithms are used for encrypting data to convert it into unintelligible form for the purpose of transmitting it over the network. These algorithms are the way to safeguard data from the hackers or intruders. The strength of an algorithm is measured by seeing how secure it is against the various security attacks. IDEA (international data encryption algorithm) is a symmetric block cipher which was developed by James Massey and Xuejia lai at Swiss Federal Institute of Technology. The plain text is processed in 64 bit block in total of 9 rounds (8 full rounds +1 output transformation round).A 128 bit key is used to generate 52 sub-keys of 16 bits each.6 sub-keys are used in each round for encryption other than last (output transformation round) IDEA has the following two main characteristics that relate to its cryptographic strength:

Confusion: The cipher text should be dependent on plaintext and key in a complicated and involved manner i.e. the relationship between the cipher text and key is made more complex. This is done in IDEA by using the following three operations:

- Bit by Bit exclusive OR ($\oplus$)
- Addition of Integer modulo 2^{16}($\boxplus$)
- Multiplication of integers modulo ($2^{16}+1$) ($\odot$)

Diffusion: Diffusion means making the relationship between cipher text and plain text is made more complex. The spreading out of a single plain text bit over many cipher text bits hides the statistical structure of the plain text. In IDEA [3, 4] diffusion is provided by a multiplicative additive block (MA block)

II. S-IDEA

Large numbers of weak class of keys were found for IDEA (International Data Encryption Algorithm). Also a new attack on round 6 of IDEA has been detected. The paper discusses the increase in strength of the present algorithm to make it more secure. There are basically two prepositions to increase the strength; firstly, by increasing the key size and secondly, by increasing the amount of diffusion. The proposed work is reflected in modified design of S-IDEA and also in the software implementation of the algorithm. The basic aim of the algorithm is to increase the strength of existing IDEA [7, 8] algorithm by exploiting its properties of confusion and diffusion. By increasing the amount of confusion as well as diffusion the algorithm can be made more powerful and less susceptible to cryptanalysis.

A new algorithm-*SECURE-INTERNATIONAL DATA ENCRYPTION ALGORITHM(S-IDEA)* is introducing significant changes that enhance algorithm's security. A detailed design of the new algorithm has been discussed. The following are the ***key design features*** of S-IDEA which distinguishes it from current IDEA algorithm:

- **Block size** - 128 bits which is divided into eight 16 bits blocks on which functions of individual sub-keys is applied.
- **No. of rounds** - 8 full rounds
  - 1 output transformation round
- **Key length** - 256 bits
- **No. of sub keys** - 104
- **Size of each sub key** - 16 bits
- 12 sub keys are used in each round

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 6, June 2012

- Two MA blocks are used in each round as compared to one in each round previously.

The following articles of present the detailed version of new design of S-IDEA along with many mathematical derivations that validates the consistency and correctness of the algorithm.

III. PROPOSED WORK

The basic aim is to increase the strength of existing IDEA encryption algorithm [7, 8]. This is required to be done because a new attack on later rounds (such as round 6) has been detected. Therefore one can suggest the following prepositions to enhance the security of the algorithm:

- ***Increasing Key size:*** The Present key size_is 128 bits. The paper proposes to increase the key size to 256 bits. Increasing the key size will add more complexity algorithm and prevent the earlier mentioned forms of attacks.
- ***Increasing the level of Diffusion*:** As defined earlier, it is the process of making the relationship between Plain Text and Cipher text more complicated & complex. Currently diffusion is provided with the help of MA (Multiplicative Additive) Block. It is used once in each round. In the proposed scenario MA Blocks could be used twice in each round, thus increasing the level of diffusion.

A.DESIGN IMPLEMENTATION OF S-IDEA: - With a slight modification in the present algorithm one can increase the cryptographic strength of algorithm. In the modified version, the proposed data is to be processed in 128 bit blocks. The 128 bit block is divided into eight 16-bit blocks on which functions of individual sub-keys is applied. The algorithm still consists of 8 rounds plus 1 output transformation round; but now 12 sub-keys are used in each round - 8 in transformation round and 4 in sub-encryption round. The last round uses 8-keys. In total 104 sub-keys are used in 8+1 rounds. At the last round the eight 16- bit blocks are recombined to form a 128 bit cipher text block. The block diagram of improved IDEA is given in fig.1.

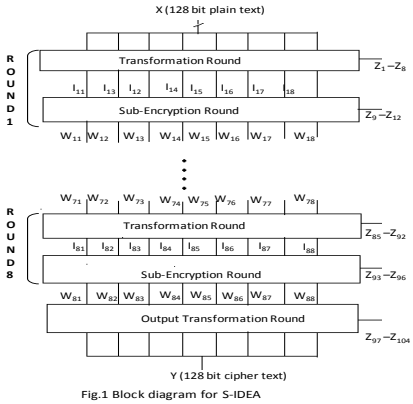

Fig.1 Block diagram for S-IDEA

Fig 1 Block diagram of S-IDEA

B. SUBKEY GENERATION

- The sub-key generation process is kept same as previously with a difference that now 256 bit key is used.
- The first 16 sub-keys are generated directly from 256 bit key, where Z_1 is equal to first (most significant) 16 bits,Z_2 equal to next 16 bits , and so on.
- After that 25 bit circular left shift is applied to the key and next 16 sub-keys are generated as described above.
- This process of sub-key generation is continued till all 104 sub-keys are generated. Diagrammatically it is shown in fig.2. The Sub-keys used in each round is given in Table.1 (see at the end)

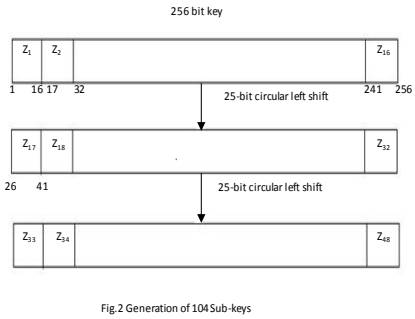

Fig.2 Generation of 104 Sub-keys

Fig 2 Generation of 104 subkey

C. ENCRYPTION OF S-IDEA

- The 128 bits text is processed in 8 block of 16 bit each.
- The proposed modified version of IDEA(S-IDEA) can be seen as two sub-block of 64 bits running in parallel with each other. Each round in encryption uses two MA block and 12 keys.
- Each round consists of two further divisions i.e. Transformation followed by Sub-Encryption, transformation in each round uses 8 keys whereas sub-encryption uses 4 keys.
- The former description of keys is valid for round from 1 to 8 where as the 9th round called the Output transformation round uses 8 keys.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 6, June 2012

- The structural detail of round 1 is depicted in fig.3. The output transformation round is depicted in fig.4.

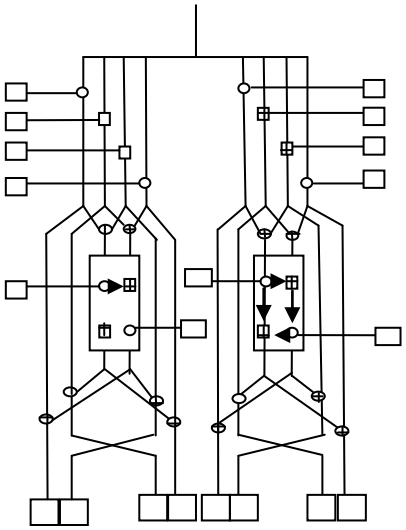

Fig 3 Structural details of round 1

From fig.1and fig.3 following relations can be written:

- $W_{11}=I_{11} \oplus MA_{R1}(I_{11} \oplus I_{13}, I_{12} \oplus I_{14})$
- $W_{12}=I_{13} \oplus MA_{R1}(I_{11} \oplus I_{13}, I_{12} \oplus I_{14})$
- $W_{13}=I_{12} \oplus MA_{L1}(I_{11} \oplus I_{13}, I_{12} \oplus I_{14})$
- $W_{14}=I_{14} \oplus MA_{L1}(I_{11} \oplus I_{13}, I_{12} \oplus I_{14})$
- $W_{15}=I_{15} \oplus MA_{R2}(I_{15} \oplus I_{17}, I_{16} \oplus I_{18})$
- $W_{16}=I_{17} \oplus MA_{R2}(I_{15} \oplus I_{17}, I_{16} \oplus I_{18})$
- $W_{17}=I_{16} \oplus MA_{L2}(I_{15} \oplus I_{17}, I_{16} \oplus I_{18})$
- $W_{18}=I_{18} \oplus MA_{L2}(I_{15} \oplus I_{17}, I_{16} \oplus I_{18})$
- $W_{81}=I_{81} \oplus MA_{R1}(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})$
- $W_{82}=I_{83} \oplus MA_{R1}(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})$
- $W_{83}=I_{82} \oplus MA_{L1}(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})$
- $W_{84}=I_{84} \oplus MA_{L1}(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})$
- $W_{85}=I_{85} \oplus MA_{R2}(I_{85} \oplus I_{87}, I_{86} \oplus I_{88})$
- $W_{86}=I_{87} \oplus MA_{R2}(I_{85} \oplus I_{87}, I_{86} \oplus I_{88})$
- $W_{87}=I_{86} \oplus MA_{L2}(I_{85} \oplus I_{87}, I_{86} \oplus I_{88})$
- $W_{88}=I_{88} \oplus MA_{L2}(I_{85} \oplus I_{87}, I_{86} \oplus I_{88})$

The following relations can be seen from fig.4:

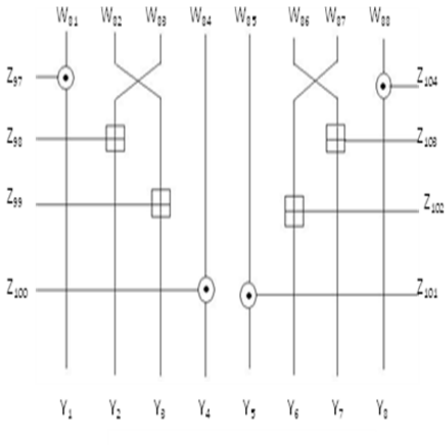

Fig 4 Output transformation round

Table.1 Generation of encryption sub-keys

- $Y_1=W_{81} \odot Z_{97}$
- $Y_2=W_{83} \boxplus Z_{98}$
- $Y_3=W_{82} \boxplus Z_{99}$
- $Y_4=W_{84} \odot Z_{100}$
- $Y_5=W_{85} \odot Z_{101}$
- $Y_6=W_{87} \boxplus Z_{102}$
- $Y_7=W_{86} \boxplus Z_{103}$
- $Y_8=W_{88} \odot Z_1$

D. DECRYPTION OF S-IDEA

The decryption process is same as encryption process .The output of each round is denoted by V whereas the intermediate output undergoing transformation in each round is denoted by J. The overall structure of decryption is exactly the same as in fig.3.with a difference that different sub-keys are used. The relations of Decryption sub-keys to Encryption sub-keys is depicted in Table.2

The ***Decryption Sub-keys are related to the Encryption sub-keys*** as follows:

1. The first eight sub-keys of encryption of round i are derived from the first eight sub-keys of decryption round (10-i) and vice versa.
2. The first and fourth, fifth and eighth sub-keys of encryption of round i are equal to the multiplicative inverse modulo $(2^{16}+1)$ of the corresponding to the first and fourth, fifth and eighth sub-keys of decryption of round (10-i) and vice versa.
3. For round 2 through 8, the second, third, sixth and seventh sub-keys of decryption are equal to additive inverse modulo (2^{16}) of the corresponding third, second, seventh and sixth sub-keys of encryption round (10-i).

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 6, June 2012

4. For round 1 and 9, the second, third, sixth and seventh sub-keys of decryption are equal to additive inverse modulo (2^{16}) of the corresponding second, third, sixth and seventh sub-keys of encryption round (10-i).
5. For the first eight rounds, the ninth, tenth, eleventh and twelfth sub-keys of decryption round i are equal to the ninth, tenth, eleventh and twelfth sub-keys of encryption round (9-i).

1 RELATION BETWEEN J AND W

The output of transformation round of decryption (J) is related to output of sub-encryption round of encryption (W) and vice versa. Consider the fig.5.We can write the following relations:

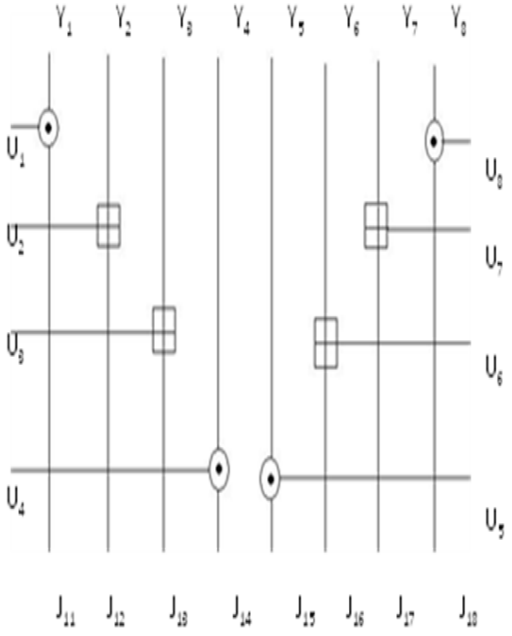

Fig 5 Decryption (transformation round) round 1

Table.2 Relation between encryption and decryption sub-keys

- $Y_1=W_{81} \odot Z_{97}$
- $Y_2=W_{83} \boxplus Z_{98}$
- $Y_3=W_{82} \boxplus Z_{99}$
- $Y_4=W_{84} \odot Z_{100}$
- $Y_5=W_{85} \odot Z_{101}$
- $Y_6=W_{87} \boxplus Z_{102}$
- $Y_7=W_{86} \boxplus Z_{103}$
- $Y_8=W_{88} \odot Z_{104}$

$V_{15}=W_{85} \oplus MA_{R2}(W_{85} \oplus W_{86}, W_{87} \oplus W_{88})$

Substituting the values of W_{85} ,W_{86}, W_{87} ,W_{88} :

$V_{15} = [I_{85} \oplus MA_{R2}(I_{85} \oplus I_{87}, I_{86} \oplus I_{88})] \oplus$

$MA_{R2}[I_{85} \oplus MA_{R2}(I_{85} \oplus I_{87}, I_{86} \oplus I_{88})]$

Substituting Y_1 in the equation corresponding to J_{11}:

$J_{11}=Y_1 \odot U_1$

$= W_{81} \odot Z_{97} \odot U_1$

$= W_{81} \odot Z_{97} \odot Z_{97}^{-1}$ $(U_1=Z_{97}^{-1})$

$= W_{81} \odot 1$

$J_{11} = W_{81}$

Substituting Y_2 in the equation corresponding to J_{12}:

$J_{12}=Y_2 \boxplus U_2$

$= W_{83} \boxplus Z_{98} \boxplus U_2$

$= W_{83} \boxplus Z_{98} \boxplus -Z_{98}$ $(U_2= -Z_{98})$

$= W_{83} \boxplus 0$

$J_{12} = W_{83}$

Similarly we can derive the following equivalences:

Table.3 Relation between J and W

$J_{11}=W_{81}$	$J_{15}=W_{85}$
$J_{12}=W_{83}$	$J_{16}=W_{87}$
$J_{13}=W_{82}$	$J_{17}=W_{86}$
$J_{14}=W_{84}$	$J_{18}=W_{88}$

RELATION BETWEEN V AND I

We can write V in decryption corresponding to W in encryption as follows:

$V_{11}=J_{11} \oplus MA_{R1}(J_{11} \oplus J_{13}, J_{12} \oplus J_{14})$

$V_{12}=J_{13} \oplus MA_{R1}(J_{11} \oplus J_{13}, J_{12} \oplus J_{14})$

$V_{13}=J_{12} \oplus MA_{L1}(J_{11} \oplus J_{13}, J_{12} \oplus J_{14})$

$V_{14}=J_{14} \oplus MA_{L1}(J_{11} \oplus J_{13}, J_{12} \oplus J_{14})$

$V_{15}=J_{15} \oplus MA_{R2}(J_{15} \oplus J_{17}, J_{16} \oplus J_{18})$

$V_{16}=J_{17} \oplus MA_{R2}(J_{15} \oplus J_{17}, J_{16} \oplus J_{18})$

$V_{17}=J_{16} \oplus MA_{L2}(J_{15} \oplus J_{17}, J_{16} \oplus J_{18})$

$V_{18}=J_{18} \oplus MA_{L2}(J_{15} \oplus J_{17}, J_{16} \oplus J_{18})$

Consider the following equation:

$V_{15}=J_{15} \oplus MA_{R2}(J_{15} \oplus J_{17}, J_{16} \oplus J_{18})$

Substituting the values of J_{15} , J_{16} , J_{17} , J_{18} :

$\oplus I_{87} \oplus MA_{R2}(I_{85} \oplus I_{87}, I_{86} \oplus I_{88})$,

$I_{86} \oplus MA_{L2}(I_{85} \oplus I_{87}, I_{86} \oplus I_{88})$

$\oplus I_{88} \oplus MA_{L2}(I_{85} \oplus I_{87}, I_{86} \oplus I_{88})]$

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 6, June 2012

$V_{15} = [I_{85} \oplus MA_{R2}(I_{85} \oplus I_{87}, I_{86} \oplus I_{88})]$
$\oplus MA_{R2}[I_{85} \oplus I_{87}, I_{86} \oplus I_{88}]$
$V_{15} = I_{85} \oplus 0$
$V_{15}=I_{85}$

nt to	Z_{-1}	8	9	Z_{0}^{-1}	Z_{1}^{-1}	2	3	Z_{4}^{-1}	3			

Round 2

Round 1	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7	Z_8	Z_9	Z_{10}	Z_{11}	Z_{12}
Round 2	Z_{13}	Z_{14}	Z_{15}	Z_{16}	Z_{17}	Z_{18}	Z_{19}	Z_{20}	Z_{21}	Z_{22}	Z_{23}	Z_{24}
Round 3	Z_{25}	Z_{26}	Z_{27}	Z_{28}	Z_{29}	Z_{30}	Z_{31}	Z_{32}	Z_{33}	Z_{34}	Z_{35}	Z_{36}
Round 4	Z_{37}	Z_{38}	Z_{39}	Z_{40}	Z_{41}	Z_{42}	Z_{43}	Z_{44}	Z_{45}	Z_{46}	Z_{47}	Z_{48}
Round 5	Z_{49}	Z_{50}	Z_{51}	Z_{52}	Z_{53}	Z_{54}	Z_{55}	Z_{56}	Z_{57}	Z_{58}	Z_{59}	Z_{60}
Round 6	Z_{61}	Z_{62}	Z_{63}	Z_{64}	Z_{65}	Z_{66}	Z_{67}	Z_{68}	Z_{69}	Z_{70}	Z_{71}	Z_{72}
Round 7	Z_{73}	Z_{74}	Z_{75}	Z_{76}	Z_{77}	Z_{78}	Z_{79}	Z_{80}	Z_{81}	Z_{82}	Z_{83}	Z_{84}
Round 8	Z_{85}	Z_{86}	Z_{87}	Z_{88}	Z_{89}	Z_{90}	Z_{91}	Z_{92}	Z_{93}	Z_{94}	Z_{95}	Z_{96}
Round 9	Z_{97}	Z_{98}	Z_{99}	Z_{100}	Z_{101}	Z_{102}	Z_{103}	Z_{104}				

Similarly we can derive the following equivalences:

$V_{11}=I_{81}$	$V_{15}=I_{85}$
$V_{12}=I_{83}$	$V_{16}=I_{87}$
$V_{13}=I_{82}$	$V_{17}=I_{86}$
$V_{14}=I_{84}$	$V_{18}=I_{88}$

Table.4 Relation between V and I

Round 1

De.Sub-keys	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8	U_9	U_{10}	U_{11}	U_{12}
Equivale	Z_{97}	$-Z_{9}$	$-Z_{9}$	Z_{10}	Z_{10}	$-Z_{10}$	$-Z_{10}$	Z_{10}	Z_{9}	Z_{94}	Z_{95}	Z_{96}

De.Sub-keys	U_{13}	U_{14}	U_{15}	U_{16}	U_{17}	U_{18}	U_{19}	U_{20}	U_{21}	U_{22}	U_{23}	U_{24}
Equivalent to	Z_{85}^{-1}	$-Z_{87}$	$-Z_{86}$	Z_{88}^{-1}	Z_{89}^{-1}	$-Z_{91}$	$-Z_{90}$	Z_{92}^{-1}	Z_{81}	Z_{82}	Z_{83}	Z_{84}

Round 3

De.Sub-keys	U_{25}	U_{26}	U_{27}	U_{28}	U_{29}	U_{30}	U_{31}	U_{32}	U_{33}	U_{34}	U_{35}	U_{36}
Equivalent to	Z_{73}^{-1}	$-Z_{75}$	$-Z_{74}$	Z_{76}^{-1}	Z_{77}^{-1}	$-Z_{79}$	$-Z_{78}$	Z_{80}^{-1}	Z_{69}	Z_{70}	Z_{71}	Z_{72}

Round 4

De.Sub-	U_{37}	U_{38}	U_{39}	U_{40}	U_{41}	U_{42}	U_{43}	U_{44}	U_{45}	U_{46}	U_{47}	U_{48}

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 6, June 2012

keys												
Equivalent to	Z_{61}^{-1}	$-Z_{63}$	$-Z_{62}$	Z_{64}^{-1}	Z_{65}^{-1}	$-Z_{67}$	$-Z_{66}$	Z_{68}^{-1}	Z_{57}	Z_{58}	Z_{59}	Z_{60}

Round 5

De.Sub-keys	U_{49}	U_{50}	U_{51}	U_{52}	U_{53}	U_{54}	U_{55}	U_{56}	U_{57}	U_{58}	U_{59}	U_{60}
Equivalent to	Z_{49}^{-1}	$-Z_{51}$	$-Z_{50}$	Z_{52}^{-1}	Z_{53}^{-1}	$-Z_{55}$	$-Z_{54}$	Z_{56}^{-1}	Z_{45}	Z_{46}	Z_{47}	Z_{48}

Round 6

De.Sub-keys	U_{61}	U_{62}	U_{63}	U_{64}	U_{65}	U_{66}	U_{67}	U_{68}	U_{69}	U_{70}	U_{71}	U_{72}
Equivalent to	Z_{37}^{-1}	$-Z_{39}$	$-Z_{38}$	Z_{40}^{-1}	Z_{41}^{-1}	$-Z_{43}$	$-Z_{42}$	Z_{44}^{-1}	Z_{33}	Z_{34}	Z_{35}	Z_{36}

Round 7

De.Sub-keys	U_{73}	U_{74}	U_{75}	U_{76}	U_{77}	U_{78}	U_{79}	U_{80}	U_{81}	U_{82}	U_{83}	U_{84}
Equivalent to	Z_{25}^{-1}	$-Z_{27}$	$-Z_{26}$	Z_{28}^{-1}	Z_{29}^{-1}	$-Z_{31}$	$-Z_{30}$	Z_{32}^{-1}	Z_{21}	Z_{22}	Z_{23}	Z_{24}

Round 8

De.Sub-keys	U_{85}	U_{86}	U_{87}	U_{88}	U_{89}	U_{90}	U_{91}	U_{92}	U_{93}	U_{94}	U_{95}	U_{96}
Equivalent to	Z_{13}^{-1}	$-Z_{15}$	$-Z_{14}$	Z_{16}^{-1}	Z_{17}^{-1}	$-Z_{19}$	$-Z_{18}$	Z_{20}^{-1}	Z_{9}	Z_{10}	Z_{11}	Z_{12}

Round 9

De.Sub-keys	U_{97}	U_{48}	U_{99}	U_{100}	U_{101}	U_{102}	U_{103}	U_{104}				
Equivalent to	Z_1^{-1}	$-Z_2$	$-Z_3$	Z_4^{-1}	Z_5^{-1}	$-Z_6$	$-Z_7$	Z_8^{-1}				

IV. CONCLUSION

- The S-IDEA aims at increasing the complexity of the existing IDEA algorithm. To do so it exploits the properties of confusion and diffusion employed in the algorithm. The proposed algorithm (S-IDEA)has two key features:
  -increased key size (256 bits)
  -increased degree of diffusion (two MA blocks are used in a single round instead of one)
- By increasing the key size the exhaustive key search becomes practically infeasible .Also, now 104 sub-keys are being used as compared to 52 sub-keys previously which enhances the complexity of confusion. Therefore the probability of other forms of attack is reduced due to amount of work that has to be carried out when 104 sub-keys are involved.
- Addition of a new MA block in each round of IDEA has contributed to an increase in complexity of diffusion. It makes the algorithm more secure and less susceptible to cryptanalysis.
- This cipher structure will provide confusion and diffusion and will facilitate both hardware and software implementation.
- The implementation of S-IDEA using C language is provided which certifies the correctness and validity of the algorithm

REFERENCES

[1] Garfinkel, Simson (December 1, 1994). PGP: Pretty Good Privacy. O'Reilly Media. pp. 101–102. ISBN 978-1565920989.

[2] Biham, E.; Dunkelman, O.; Keller, N. "A New Attack on 6-Round IDEA". Springer-Verlag.

[3] Daemen, Joan; Govaerts, Rene; Vandewalle, Joos (1993), "Weak Keys for IDEA", Advances in Cryptology, CRYPTO 93 Proceedings: 224–231

[4] Nakahara, Jorge Jr.; Preneel, Bart; Vandewalle, Joos (2002), A note on Weak Keys of PES, IDEA and some Extended Variants

[5] Biryukov, Alex; Nakahara, Jorge Jr.; Preneel, Bart; Vandewalle, Joos, "New Weak-Key Classes of IDEA", Information and Communications Security, 4th International Conference, ICICS 2002

[6] Strength Assessment of Encryption Algorithms-- Limor Elbaz & Hagai Bar-El (White Paper).

[7] Thaduri, M., Yoo, S.M and Gaede, R.,"An efficient implementation of IDEA encryption algorithm using VHDL", 2004 Elsevier.

[8] Rahul Ranjan, I.Poonguzahli, "VLSI Implementation of IDEA Encryption Algorithm", Mobile and Pervasive Computing (CoMPC-2008).

[9] Webpage www.finecrypt.com,"The IDEA encryption algorithm".

[10] Lai, X. and Massey, J., "A proposal for a new block encryption standard,"Proceedings, Eurocrypt"90, 1990.