QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

A Proposed Non Feistel Block Cipher Algorithm

Ahssan Ahmed Mohammed
Department of software, College IT, University of Babylon - Iraq
ahssan_ahsan@yahoo.com

Dr.Abdulkareem O. Ibadi
Department Computer Engineering, Baghdad College for Economic Sciences University - Iraq
dr.ibadi@yahoo.com

ARTICALE INFO

Article History:

Received: 13 March 2017

Accepted: 1 April 2017

Published: 10 April 2017

DOI: 10.25212/lfu.qzj.2.2.09

Keywords: *Encryption, Decryption, Block cipher, Keys, SubKey, Map Function, Wave Function, Permutation.*

ABSTRACT

In this work, A proposed block cipher algorithm is designed with multiple of 32 bits as a length of block performed in heterogonous multiple block cipher dependent on the application field , Multiple of 48 bits as a key length are entered automatically used in variable permutation, addition function and xor operation. A proposed algorithm performed in single round to giving fast and high security algorithm used in different Purposes. Another proposed functions for different purpose such as Balance Function between balance fixed number and initial permutation and inverse initial permutation, Maps function as lookup table (map2,map3,map4 and map5). Wave Function as a nonlinear function of 8-bits of input and same for the output. This algorithm can be designed in several blocks length depends on the application field, increase speed, higher complexity and for reduction of cost.

1. INTRODUCTION

Encryption Operation is the process of converting a original data called plaintext into ciphertext using secret key, and can be convert back into the original data with the same secret key. There are several kinds of data encryption schemes which form the fundamental of security. [1]

Encryption Operation schemes are generally based on either block cipher or stream cipher. Historically for providing confidentiality should be Encryption focus on symmetric encryption. It is only in the last several decades that other considerations, such as Integrity, Authentication and Digital Signature have been included in cryptology theory and it practice. The security of the data basically depends on two laborer first one is Confidentiality and second one is Authentication. Achieving confidentiality means the data is encrypting bulk digital data used block cipher. Single round of encryption offers inadequate security but multiple rounds offer increasing security but the side effect is time consumed not always, it is dependent on the strength and security of encryption functions used .[2]

The proposed algorithm is different of another by used block length multiple of 32 bits as a homogenous block cipher (4-8-12-16 bytes) with multiple of 48 bits of key and 4

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

nonlinearity Maps(Map2, Map3,Map4 Map5) all of them processing in one round and new subkey generation algorithm also been designed new function for generated permutation array used as initial permutation and inverse initial permutation then reversible variable permutation dependent on secret key value as well Wave function is a nonlinear function.

Cryptography is one of many aspects of security, It is science and art of writing. Egyptian Hieroglyphs in an inscription is first used of cryptography in 1900 B.C. The primary functions of cryptography are confidentiality, Privacy, Authentication, Integrity, Non-repudiation and Key exchange.[3]

The three types of Cryptography algorithms are :

1- Secret Key Cryptography or symmetric encryption : Used a single key for both encryption and decryption, Primarily used for confidentiality and privacy.
2- Public Key Cryptography or asymmetric encryption: Used two keys, one of them for encryption and another for decryption, mostly used for key exchange, non-repudiation and authentication .
3- Hash Function: Used a mathematical transformation to encrypt of information, providing a digital fingerprint. mostly used for message integrity.

Secret key cryptography algorithms in general categorized as being either stream cipher or block cipher algorithms will focus on this aspect in our proposal. Stream ciphers operated on a one bit at a time and key is continuously changed, means the Encryption Operation of each digit depends on the current state of the cipher engine, Stream cipher is also call state cipher. Generally, single bit/bites are used as single digits to avoid concerns of security . Error propagation is a problem of the Stream cipher as a bit corrupted in transmission will result of corrupted set of bits at the receiving side.[4]

Block Cipher Encrypts/Decrypts one block from data at a time used the same key on each block with fixed block/key length. Encryption key scheme is determines the order in which Transportation, Substitution and other mathematical functions are applied on each block. Block cipher algorithms used two operations are Confusion and Diffusion to encrypt Plaintext Block into Ciphertext Block. The aim of confusion is to make the relationship among the encryption key and the ciphertext as complex as possible. Ideally, every bit in the key should influence in every bit of the Ciphertext Block. By contrast, Diffusion operation propagates the influence of each bit in the Plaintext Block over several bites in the Ciphertext Block, making the cipher few oversensitive to statistical attacks.[6]

The actuality that stream cipher data Encryption/Decryption single bit at a time means that they are particularly well appropriate to real time hardware applications, like image , video and audio applications. Stream cipher algorithm is practical weaker and less efficient than block cipher algorithm for software applications and it minimal frequently used in that sphere. Block cipher algorithm is easier to implement in Software application because the message encrypted in blocks length that software already uses. The Encryption key is predominantly the same size as the block length. Hence block ciphers achieve higher diffusion and error propagation than stream ciphers, although it is worth noting that the algorithm determines the amount of diffusion.[4][5]

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Block ciphers algorithms usually require large memory, because they perform on larger data chunks and predominating have carry over from preceding blocks, whilst Stream ciphers algorithms perform on only a fewest bits or byte at a time they have relatively less memory requirements and therefore cheaper to implement in limited scenarios like firmware, embedded devices and special hardware.[5]

Stream ciphers algorithms are more difficult to perform appropriate, and apt to weaknesses based on usage, since the fundaments are similar to one time pad, the key stream cipher has more stringent requirements.[4]

On the other hand, Block ciphers algorithms encrypt a whole block at a time and moreover have feedback modes which are most recommended, they are over sensitive to noise in transmission, means if you mess up one data part, all the remnant is maybe unrecoverable. while stream ciphers algorithms bytes are individually encrypted with no connection to other data chunks in most ciphers/modes, and typically have support for interruptions on the line.[5]

Stream ciphers algorithms do not provide security authentication or integrity protection, but some block ciphers algorithms can provide integrity protection and confidentiality depending on mode.[4][5]

The reason for choosing Block ciphers in this proposed because more useful when the data amount is pre known such as a data file, fields, or request protocols.

2. A PROPOSED BLOCK CIPHER

A proposed block cipher algorithm is a based on Non-Feistel Block Cipher algorithms. The block diagram of it is shown in figure(1) and the algorithm is given in the following eight steps

Algorithm:

INPUT : block of length 32 bits, key of length 48 bits.
OUTPUT: block of length 32 bits.

1. Compute 32 bits after initial permutation by balance function = P block Xor balance constant block.
2. Compute addition operation on balance block and subkey1 to yield P sum block (each 8 bits of balance block addition to a single 8 bits of subkey1).
3. Perform Map Function on P-sum block to convert each 8 bits to covalence bits.
4. Perform variable permutation on P-Map block based on bits location of key.
5. Perform Reversible Wave function on variable permutation block.
6. Shifting and Rotation operations for each 8 bits of wave block.
7. Compute Xor operation on each 8 bits of block with different 8 bits of subkey2.
7. Swap among each 8 bits of block to produce the C block of length 32 bits.
8. Next 32 bits.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

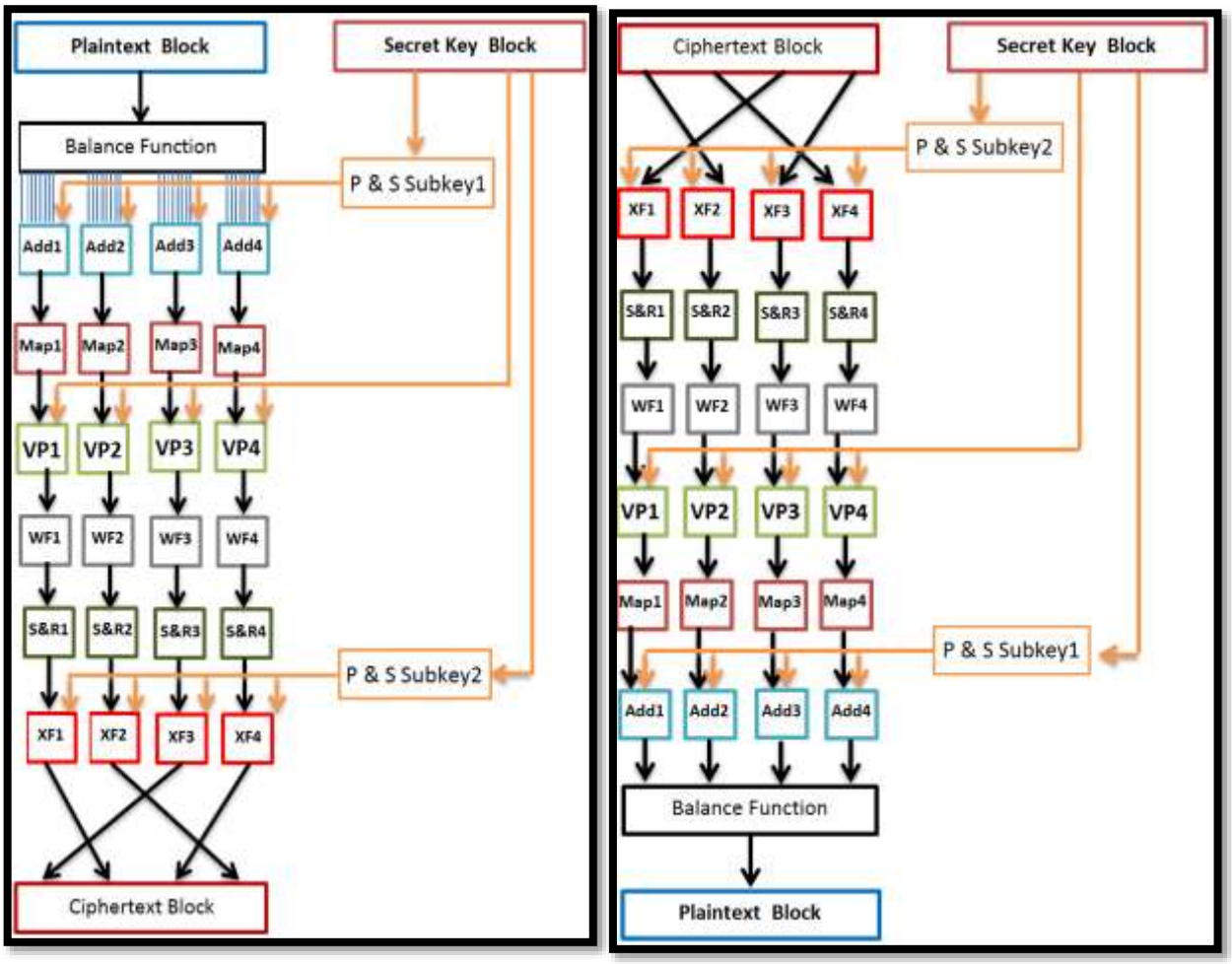

Figure: 1 Illustrate Encryption & Decryption algorithm structure

The main idea of a proposed block cipher algorithm is begin by input block of plaintext and the output is block of ciphertext after executed in number of different steps.

The algorithm has a multiple of 32-bits block size and multiple of 48 bits key length. It is a 7-step built based on non Feistel cipher algorithm. The blocks are constructed by converting a characters into 32 bits by using ASCII and also entered key by converting a 6-character into 48 bits by using ASCII for each character. The figure 2&3 illustrate encryption and decryption steps structure.

2.1. BALANCE FUNCTION

Two main functions are operate in Balance function they are : Initial permutation and XOR function, The input/output of the Balance function is a block of length 32 bits, the input block permutated in permutation generation algorithm to generate initial permutation (IP) as in table 1 and inverse permutation (IP^{-1}) as in table 2 for first function then Xor-ed with a block of balance constant of the same length. The block diagram of it is shown in figure 2

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
4	11	24	13	9	16	3	17	8	14	2	20	19	0	26	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
10	7	18	27	12	23	6	25	31	28	1	21	30	5	29	22

Table 1 : Initial Permutation IP

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
13	26	10	6	0	29	22	17	8	4	16	1	20	3	9	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
5	7	18	12	11	27	31	21	2	23	14	19	25	30	28	24

Table 2 : Inverse Initial Permutation IP^{-1}

2.1.1 PERMUTATION GENERATION ALGORITHM

Input : list of number schedule arranged from 0 to n-1
Output: array of random numbers between 0 to n-1 without repetition
1. Loop from 0 to n-1 .
2. Using predefined random function in vb.net (Random) working storage area.
3.Using list operation to move location of random number generated to the output array
4. Remove the location and reduce list length by one .
5. Next.

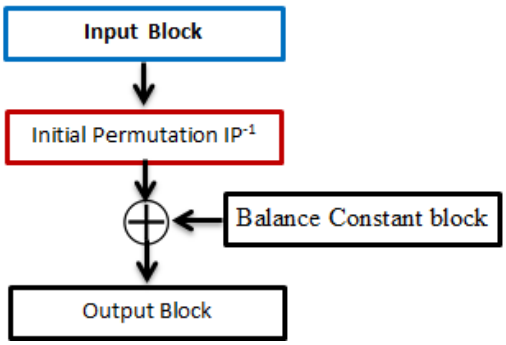

Figure 2: Illustrate Balance Function structure

2.2. ADDITION FUNCTION

Addition operation is second function of a proposed block cipher algorithm. The output block of Balance function will dividing into set of 8-bits each one will addition with single 8-bits of subkey1 block as performed by used permutation and selection for the secret key as shown in table 3.

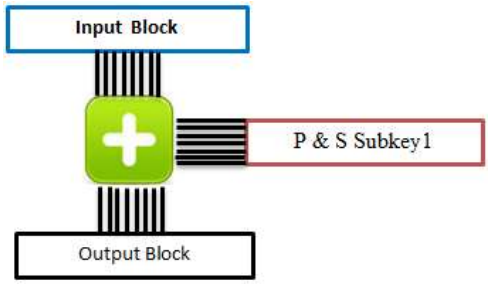

Figure 3: Illustrate Addition Function structure

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
47	31	22	38	29	1	10	45	41	36	16	12	37	28	17	2
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
9	15	32	3	39	19	6	18	7	14	26	8	24	40	34	33

Table 3 : Permutation and Selection of Subkey1

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

2.3. MAP FUNCTION

Map function is performed for a byte of input block, A proposed block cipher used 4 maps each one has a different number. Different permutation is present after each Map to help for bits propagation and diffusion increased with high complexity.

2.3.1 Map Function generation

Map generated by converted the input byte into complement number excepted the bits has location equal to the random value generate between 0 -7. A proposed block cipher used 4 maps each one with different number of excepted bits (Map2 means two bits has generated and so on for Map3, Map4 and Map5). Maps function structure is shown in figure 4. Table 4 is example of Maps function.

	Input	Random Values	Output
Map2	10001110	2-4	01011001
Map3	10010011	3-4-7	01110101
Map4	10011000	0-1-6-7	10100100
Map5	10011101	0-1-2-3-4	10011010

Table 4 : Example of Maps Function

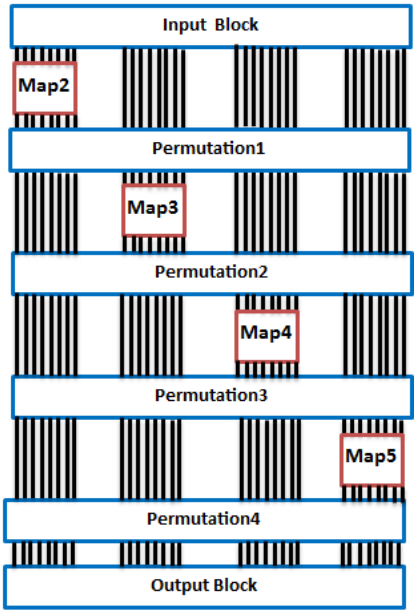

Figure 4 : Maps Function structure

2.4. REVERSIABLE VARIABLE PERMUTATION

Variable permutation is a reversible function, it relying to secret key values. Variable permutation performed for each byte of block dependent on location of secret key bits. The variable permutation is implement by three levels as shown in figure 3. Level one check the secret key and make swapping between two neighboring bits when the read bit is one. Level two and three perform swapping between widely bits as shown in following structure to guarantee permute from first to last bit.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

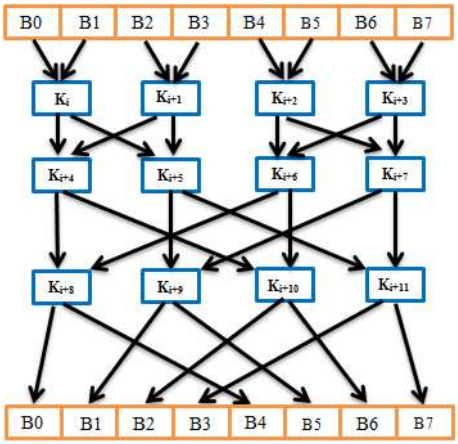

Figure 5 : Reversible Variable Permutation(VP) structure

2.5. WAVE FUNCTION

The wave function is a nonlinear function designed to be of the same size inputs and outputs which help to increase the confusion and diffusion of output result because whenever a zero is located in a sequence the rest of the sequence will be converted[7]. A proposed block cipher algorithm used the Wave function with byte of input and same for output. If X is the input set and Y is the output set so Y can write as Y=WF(x) where,

$Y_1=X_1 \oplus 1$
$Y_2=X_2 \oplus X_1 \oplus 1$
$Y_3= X_1 \otimes X_2 \oplus X_3 \oplus 1$
$Y_n=X_1 \otimes X_2 \otimes \ldots \otimes X_{n-1} \oplus X_n \oplus 1$

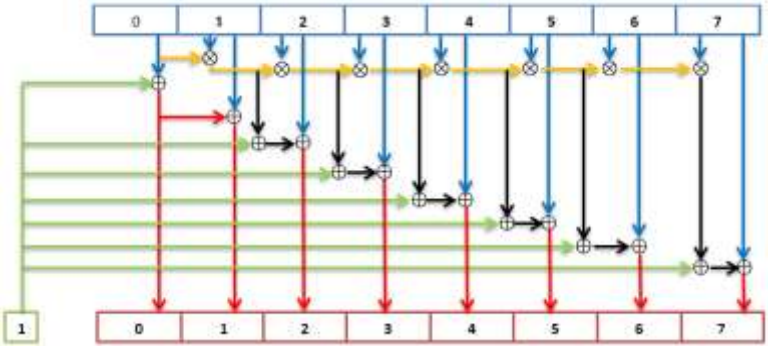

Figure 6 : Reversible Wave Function structure

Another feature of the Wave Function is that never results in the same sequence and the output will be repeated after 2^n trial.

2.6. SR FUNCTION

A Shifting and Rotation function is propagation function for each byte of block. A proposed block cipher used four shifting and rotation function (S&R1 means shifting each byte by one and so on for S&R2 , S&R3 and S&R4).

2.7. XF FUNCTION

XF function is xor operation between input block and subkey2, The input of the XF function is a block of length 32 bits Xor-ed with a block of Subkey2 of the same length generated by permutation and selection operation for secret key. In the end the output will

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

swap among each 8 bits and saving the ciphertext block in the binary file as shown in the main structure. Figure 6 illustrate XF function structure or single 8 bits

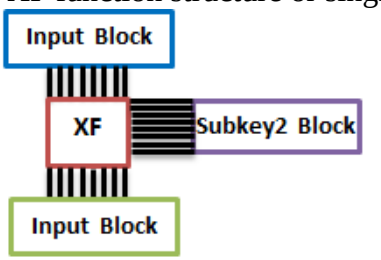

Figure 6 : Single XF function structure

2.8. KEY MANAGMENT

A proposed block cipher algorithm used multiple of 48 bits as a secret key by entered automatically dependent on application field such as password , data, image, audio, video, satellite communication its. Secret key used in variable permutation to generate permutation dependent on each bit as discussed in 4.4 . Subkeys are generated by scheduling of secret key in two operations as selection and permutation . The input of the algorithm is the secret key (6 character) witch are converted into 48 bits using ASCII code, A subkey1 and subkey2 are generated by selection and permutation of 32 bits from the 48 bits of secret key as shown in a proposed algorithm structure.

3. EVALUATION

There are two types of block cipher Feistel and Non-Feistel cipher, a feistel cipher algorithm is a block cipher construction as a symmetric build. This came on the label of a German inventor Horst Feistel. A Wide proportion of block ciphers use the Feistel network, such as the (DES) Data Encryption Standard, Blowfish, KASUMI, Simon and etc. The advantage of the Feistel Network is very similar for the encryption & decryption operations it is identical in some cases and requiring only moving from up to down ,From top to bottom or a reversal of the key schedule. Feistel ciphers and similar algorithms are product ciphers, and repeated operations for number of rounds.[5]

A non Feistel cipher is the sound type of block cipher so a Non-Feistel block cipher algorithm is a chain of linked mathematical operations performed in block cipher, it is network with a block of Plaintext and Key as inputs and applies several alternating operations to produce the ciphertext block such as AES , Square, 3-Way, SHARK , SAFER , PRESENT, and , Kuznyechik .

Although the Feistel block cipher that used S-box (like Data Encryption Standard) is fully similar to Non-Feistel block cipher, but there are some differences that make either Feistel or Non-Feistel more applicable in assured situations. For a given amount of Diffusion and Confusion, an Non-Feistel block cipher has extra inherent parallelism[11], and so given a CPU with a more number of execution units can be computed faster than a Feistel block cipher.[12] CPUs with less execution units such as most smart cards cannot take advantage of this inherent parallelism. Also Non-Feistel ciphers require s-box to be invertible (to perform decryption). Feistel inner functions have no such restriction and can be constructed as one way functions.

The advantage of a proposed algorithm is that, since its external and internal properties are change from function to function, it may be extremely difficult to find any kind of characteristic that propagates well through all of the different kinds of functions that appear in the cipher. However, implementing of a proposed algorithm and analyzing it is often much

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

more complicated. Hardware implementations are generally cheaper, and software implementations smaller and easier to correctly code.

A proposed block cipher algorithm used a balance function, These structure provide efficient implementations for mutable of the 32 bits of plaintext block by initial permutation, and used xor-ed operation with fixed balance binary number for solving problem when all plaintext block (0) or (1).

A Map function is substitutes a byte (the input of map function) by another byte (Map Function output). This Substitution should be one byte to one byte, to ensure inevitability for decryption of a proposed algorithm. The good Function goal is changing one input bit will change about half of the output bits.

The Wave Function is a reversible nonlinear function which helps to increase the confusion of the resulting output besides, it helps to increase the diffusion because whenever a zero is located in a sequence the rest of the sequence will be converted. Another feature is that never results in the same sequence and the output will be repeated after 2^n trial.

Addition operation with subkey1, Variable permutation dependent on key locations values, Shifting and Rotation operations of byte plaintext block, Xor-ed with subkey2 and Bytes Swapping operation are helps for increasing alteration among each byte.

Diffusion is important concept in the design of robust of block cipher algorithm, It is operation between plaintext block and ciphertext block means if changed one bit of plaintext block then several bits of ciphertext block should be changed and Vice versa. In another interpretation, This means the frequency statistics of bit in the plaintext block are diffused over several bits in the ciphertext block and statistical attack need more meaningful to do a ciphertext block. Table 5,6 shown the range of diffusion between plaintext block and ciphertext block in the block cipher algorithm proposed.

Block length	Key length	Diffusion Range
32	48^n	12-18
64	48^n	27-35
96	48^n	40-57
128	48^n	61-68

Table 5: shown the range of diffusion with different of block size .

Key	00000000000000000000000000000000000000000000000000	Zero	One	Diffusion
Plaintext	00000000000000000000000000000000	32	0	-
Ciphertext	00111011100111111111101001011110	10	22	
Plain	00000000000000000000000000000001	31	1	
Cipher	01011001100010010011000011011100	18	14	12
Plain	00000000000000000000000000000011	30	2	
Cipher	00110001100110111011101000111110	14	18	12
Plain	00000000000000000000000000000111	29	3	
Cipher	11010010101110101011110011101010	13	19	13
Plain	00000000000000000000000000001111	28	4	
Cipher	11011110010011011001001010110110	14	18	17
Plain	00000000000000000000000000011111	27	5	
Cipher	00010011011001010010001010110011	18	14	12
Plain	00000000000000000000000000111111	26	6	
Cipher	10110100101001001011101000111011	15	17	13

Table 6: shown the range of diffusion with same of block size .

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

4. CONCLUSION

A proposed block cipher algorithm designed to create a strong algorithm that runs in a reasonable time on presently available hardware, that is rationally easy to implement, etc. As such, a proposed algorithm design may allow us to design faster and better block cipher algorithm than we could if we limited ourselves to number of round or Non-Feistel network structures.

1- We concluded the relationship between the blocks length and hardware , It can perform multiple of 32 bits as block length as a homogenous algorithm to reduce the time of execution
2- A number of rounds should be less to speed increasing.
3- Multiple of 48 bits as a secret key should be entered automatically and it dependent on application field such as password , data, image, audio, video, satellite communication its.
4- Permutation operation should be after each map function to propagate bits in each block and increase confusion and diffusion operations.

5. REFERENCES

References must be listed in the order they were cited (numerical order). The references must not be in alphabetical order eg:

1- Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: Twine: A lightweight block cipher for multiple platforms. In Selected Areas in Cryptography - SAC 2012. LNCS, vol. 7707, pp. 339-354. Springer, Heidelberg (2013).
2- Wu, W., Zhang, L.: Lblock: A lightweight block cipher. In Applied Cryptography and Network Security - ACNS 2011. LNCS vol. 6715, pp. 327-344. Springer, Heidelberg (2011).
3- *van Tilborg, Henk C. A.; Jajodia, Sushil, eds. (2011).* Encyclopedia of Cryptography and Security. *Springer.* ISBN 978-1-4419-5905-8., p. 455.
4- *Junod, Pascal & Canteaut, Anne (2011).* Advanced Linear Cryptanalysis of Block and Stream Ciphers. *IOS Press. p. 2.* ISBN 9781607508441.
5- Chakraborty, D. & Rodriguez-Henriquez F. (2014). "Block Cipher Modes of Operation from a Hardware Implementation Perspective". In Koç, Çetin K. Cryptographic Engineering. Springer. p. 321. ISBN 9780387718163.
6- Lars R. Knudsen and John Erik Mathiassen, On the Role of Key Schedules in Attacks on Iterated Ciphers, ESORICS 2014, pp322–334
7- Dr.Abdulkareem O. Ibadi, Special Security e-Mail System , Ph.D. dissertation, University of Technology , June 2007
8- Ben Morris, Phillip Rogaway, Till Stegers. "How to Encipher Messages on a Small Domain". CRYPTO 2010.
9- *Menezes, Alfred J., Oorschot, Paul C. van; Vanstone, Scott A. (2011). Handbook of Applied Cryptography (Fifth ed.). p. 251.*
10- Christof Paar, Jan Pelzl, "The Data Encryption Standard (DES) and Alternatives", free online lectures on Chapter 3 of "Understanding Cryptography, A Textbook for Students and Practitioners". Springer, 2012.
11- "Principles and Performance of Cryptographic Algorithms" by Bart Preneel, Vincent Rijmen, and Antoon Bosselaers.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

12- "The Skein Hash Function Family" 2010 by Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, Jesse Walker page 40.
13- Sinha, S., Arya, C. (2012). Algebraic Construction and Cryptographic Properties of Rijndael Substitution Box. Defence Science Journal, 62(1).
14- Paar, C., Pelzl, J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. New York City, New York: Springer Publishing.
15- Grocholewska-Czurylo, A. (2011). Cryptographic properties of modified AES-like S-boxes.
16- Annales UMCS Informatica, AI XI(2), 37-48. DOI: 10.2478/v10065-011-0009-4.
17- Easttom, C. (2015). Modern Cryptography. New York City, New York: McGraw Hill.