ISSN 2278-7763

Survey: Block cipher Methods

Salah A. k. Albermany
Computer Science dept.
University of kufa
Salah.albermany@uokufa.edu.iq

Fatima RadiHamade
Computer Science dept.
University of kufa
Fatimar.alkhalidi@student.uokufa.edu.iq

***Abstract*—In this paper we give a short overview of Symmetric key block cipher for different algorithms presented in this field according to classified it in cryptography where we classified into categories. first, Mode of operation which is ways helped to apply block cipher to encrypt larger plaintext. second, iterated product cipher which also classified it into Feistel Network, substitution-permutation networks and Unbalanced Feistel Network.**

1. INTRODUCTION

Cryptography is the science of studying information security by provide several protocols, algorithms and strategies to protect sensitive data from unauthorized access.[1]. the main objective of cryptography is to enable two people to communicate over an insecure channel [2][3].Cryptography aims to achieve the information security requirements as privacy or confidentiality, data integrity, authentication, non-repudiation and access control [4]. Cryptography it is the most important way to protect several applications which needed to be transmit quickly with a high level of security such as images, text, voice and video[5].

Modern cryptography divided into symmetric key which uses one key in encryption and decryption, and asymmetric key (public key) which uses two different keys in encryption process. Generally symmetric key faster than asymmetric key. Using symmetric key cryptography can communicate two people during secure channel, where to contact two people across secure channel must first agree on a secret key shared in between them [6].Symmetric-key cryptography classified into stream cipher and block cipher.

In this paper will concerned with Symmetric key block cipher that operating on fixed length of bits divided into separate blocks of fixed size (for example, 32, 56, 64, 128, etc.) [7]such as DES and AES algorithm that have been designated cryptography standard.

In this paper, we will give short overview about all block cipher methods and categories in cryptography then compared among all these methods according to classified it in cryptography.

2. LITERATURE REVIEWS

Several researchers presented a survey of symmetric block cipher algorithms as E. Surya et al (2012) introduced a detailed survey on symmetric key block cipher algorithms. The researchers explain in this paper the requirements of security as privacy, integrity,

ISSN 2278-7763

authentication, non-repudiation and access control and gives the importance of each of them in the cryptography. This paper concentrated on presented brief definitions for most common encryption algorithms according to classified it in cryptography where the researchers classified algorithms in this paper into symmetric algorithms which uses one a shared key between sender and receiver such as DES, AES, triple DES and Blowfish, and asymmetric algorithms (public key algorithms) which uses two different keys such as RSA. After compared all encryption methods mentioned above the researchers prove that Blowfish algorithm uses 32-bits to 448-bits variable number and the data can encrypt16 times [8].Lars R. Knudsen (1998) illustrate a survey on block cipher key where the researchers concentrate in this paper on the main application of block ciphers and the state of the art of cryptanalysis of block ciphers. The researchers during this study explain a way to break many systems quicker than by an exhaustive search for the key [9].

3. SYMMETRIC-KEY BLOCK CIPHER

Symmetric-key block ciphers are made up of two algorithms E (Encryption) and D (Decryption) and all these algorithms takes n bits' plaintext as input and gives exactly the same number of bits as output by using k bits' secret key. Block cipher can be classified as shown in the following figure.

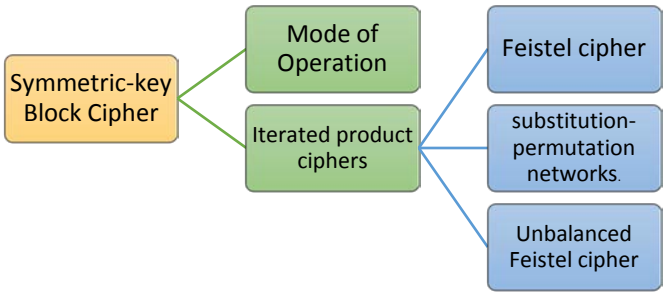

Fig1. Symmetric-Key Block Cipher categories

3.1 Mode of Operation: Literature Survey

Mode of operation ways of using block cipher for encryption, used to apply block ciphers to larger plaintexts. Mode operation classified into deterministic and probabilistic shown in figure below.

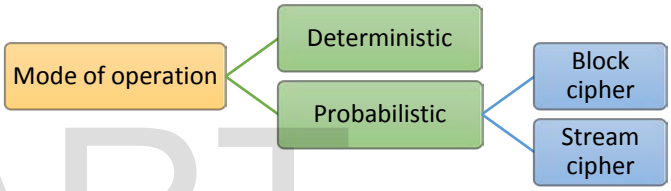

Fig2. Mode of operation category

In addition to classification above, several block cipher mode of operations designed for secrecy and authentication in a single cryptographic primitive. In this paper, we describe short overview for all types of modes presented by researchers and purpose from it. The Electronic Cod Book (ECB) is deterministic mode of operation considered the most common way in ciphering a message. This mode divided a message into number of blocks and encrypt each block in separate form from other. The main advantage of this mode, it is that the synchronization among encryption and decryption is not necessary, in this case when the receiver not received all encrypted blocks because occur problems in transmission process, the recipient can only decrypt the received blocks without any

ISSN 2278-7763

problem. ECB mode gives high speed in implementation because ECB mode operate parallel in ciphering process[10]. The Cipher Block Chaining (CBC) mode and the Cipher Feedback (CFB) mode were make the blocks of cipher text dependent on all the previous blocks of plain text through ciphering process [11]. J. Black and P. Rogaway (2002) define a new mode of operation called PMA. The new PMAC mode used for message authentication. PMAC is deterministic supported any bit length of strings, where uses single key and just max {1, [|M|/n]} block cipher calls to MAC a string M ∈ {0,1|} using an n-bit block cipher [12].P. Rogaway et al. (2003) define and describe a new parallelizable block cipher mode of operations for provides both confidentiality and authentication at the same time, the new mode called OCB mode "offset codebook". OCB encrypts string M ∈ {0, 1} using [|M|/n] +2 block-cipher where n is the block length. The main features of OCB mode it is Arbitrary-length messages and minimal-length cipher texts, Nearly optimal number of block-cipher calls, no requirement for a random IV, Efficient offset calculations and Single underlying key[13].M Bellare et al (2004) presented a new mode of operation called EAX. this mode proposed to solve the problem associated with AEAD (authenticated encryption with associated data), and EAX characterized that it's online, fixed header, and effective for removing the cost of pre-message to ciphertext [14]. Morris J. Dwork (2004) presented paper define a new mode of operation by gives recommendation for Block Cipher mode of operation. the new mode called CCM mode for symmetric key block cipher. the mode combining the techniques of two modes the counter mode and CBC-MAC algorithm. CCM used to provide the privacy and authenticity of data[15].T.Kohno et al (2004) introduce a new mode called CWC for protecting both the confidentiality and the authentication of sensitive information. CWC has manycharacteristics provable security, parallelizability, high performance in hardware and software package, and no intellectual property concerns. Based on these characteristics CWC a powerful tool for use in several performance-critical applications, CWC can processing data at 10Gbps in hardware[16]. S. Halevi and P. Rogaway (2004) illustrates in this paper a new mode for block cipher called EME where converting n-bit block cipher into mn-bits (where m belongs to [1... n]) a tweakable encryption scheme that works on strings. the new mode EME is efficient and parallelizable that used to solve the problem of disk sector encryption. the researchers proved in this paper that EME is secure for modern cryptography[17].The recently David A et al (2005) introduced a new mode for block cipher called Galois/Counter Mode (GCM) for encryption and message authentication. Galois/Counter (GCM) mode of operation has characteristics where work as a standard a lone message authentication code and accept IVs of arbitrary length also the researchers prove in this paper that GCM is secure in the standard model of security[18].Tetsu Iwata (2006) presented a new mode of operation in block cipher called CENC. CENC is Cipher -based ENCryption. CENC Is characterized by many features as highly efficient,

ISSN 2278-7763

single key, random access and etc. [19].C. Jutla (2008) define a new mode of operation called Integrity Aware Parallelizable Mode (IAPM) for block ciphers. the new mode provides both privacy and integrity of message and highly parallelizable[20]. MJO Saarinen (2011) presented a new authenticated block cipher mode of operation called Sophie Germain Counter Mode (SGCM). The new mode used with 128-bit block ciphers such as AES. SGCM is differ from Galois / Counter Mode where SGCM use GF(p) with p=2128+12451, where (p-1)/2 is also a prime, largely technically compatible alternative to GCM[21].As well as to above modes there is several modes designed to turns a block cipher into a stream ciphers such as Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR).

3.2 Iterated product ciphers

The concept of product cipher was proposed by Shannon's (1949), Shannon's define two operation of a secure cipher confusion which mean that the relationship between the plain text and cipher text is very complex, For example substitution table. and diffusion which mean the influence of one bit from plain text is a spread over many cipher text bits. For example, permutation. Combine confusion and diffusion many times to build a strong block cipher this is called product cipher [22].There are many realizations of block cipher implement according to the concept of product cipher can be classified as Feistel cipher and substitution-permutation networks etc.

3.2.1 Feistelcipher: Introduction

Feistel cipher is one of the most common structures in iterated product ciphers uses by apply round function recursively on the plain text to gives cipher text with diffusion and confusion characteristicsEncryption and decryption in the feistel cipher is similar, one of the block cipher algorithms use the scheme is Data Encryption Standard (DES) [23] [24].

3.2.1.1. Data Encryption Standard (DES)

DES is Data Encryption standard design by IBM and considered one of the most important algorithms, published by NIST and becomes a standard in 1974. DES structure consists of 64-bits input plain text and 64-bits output cipher texts and supported 56-bits key length [25].Because the encryption is process to ensure the security of transmission data across an insecure channel, and as it is known wireless channels it is an open medium to intruders and their attacks, and because the ciphering algorithms used to encrypt data in wireless networks do not take into account the bit error characteristics of the wireless channels. Zibdeh et al. (2011) presented a new modified DES algorithms (data encryption standard) to make it secure to the bit errors caused by the wireless networks. The modified algorithm improves the bit error rate (BER) performance as well as security compared to DES[26].Since the time required to cryptanalysis DES has lessened and the hardware techniques develop quickly, DES may be Vulnerable to attacked using parallel process, for this, Seung-Jo Han et al in September (1996) propose improvement into Data Encryption Standard (DES) algorithm to ensure Continuation the cryptographic security. The

ISSN 2278-7763

researchers presented new design of a DES called Improved-DES. A new algorithm processes data blocks of size 96-bits where divided the input block into 3 sub blocks of size 32-bits, increase s-boxes into 16 boxes (S1-S16) and supported key length of size 112-bits. the improved algorithm satisfying the strict avalanche criterion (SAC) and correlation coefficient.The researchers prove that the Improved-DES is stronger than the DES against differential cryptanalysis for cryptographic security and therefore the unicity distance (UD) within the Improved-DES is increased more than the DES's UD[27]. As well as to DES algorithm feistelcipher in section (3.2.1.2), we will introduce Literature survey about other methods proposed by researchers in this field of feistel cipher.

3.2.1.2. Feistel cipher: Literature survey

In addition to the DES algorithm mentioned in the previous section, several block cipher methods have been presented in the field of Feistel cipher structure. In this section, we will offer a short overview for some feistel cipher methods.Xiao-Jun Tong et al. (2015) presented a new encryption algorithm for wireless sensor network based on compound chaotic map and feistel network. the new method is block cipher key constructs a Cubic function including discretized chaotic map. in this paper the researchers prove that a new compound chaotic block cipher suitable for the wireless sensor networks, since a new block cipher has high security and efficiency, low resource depletion and this appear through tests of Security and performance of the new encryption method[28].Rashmi et al. (2015) presented a new algorithm to improve the encryption efficiency of the existing RC6 algorithm called RC7. RC7 Makes use of 6 working registers instead of 4 use in RC6 and It has a block-size of 256 bits. The new algorithm takes less time to encrypt data and it is more flexible[29]. in (2005) B. Schneier presented a new encryption algorithm of block cipher key called Blowfish, a new block cipher Blowfish processes data block of size 64-bits and supported variable key length up to 448-bits. Blowfish based on feistel cipher where including 16-round and each round consists from two parts key permutations and key-data substitution. The new algorithm suitable for application that does not change key because Blowfish algorithm not satisfying all the requirements for modern cryptographic but it is appear faster than DES (Data Encryption Standard) when implemented on 32-bit microprocessors with larger data caches [30]. Schneier et al. (1998) presented a new block cipher based on feistel network consists of 16-round with F function called TWOFISH. TWOFISH encryption algorithm processes 128-bits block size and supported key length up to 256-bits. the new algorithm can implement in hardware in 14000 gates. TWOFISH algorithm designed to satisfying NIST design criteria for AES (Advanced Encryption Standard). The main features or properties of TWOFISH that it is symmetric key block cipher, efficiency in both software and hardware for several platforms. Simple and flexible design, ease implementation and appropriate for a stream cipher, hash function and MAC [31].Ronald L. Rivest (1995) presented papers define and describe a fast symmetric

ISSN 2278-7763

block cipher key called RC5 encryption algorithm where used the same key in both encryption and decryption. RC5 algorithm variable in each of word size, number of rounds and key length. This algorithm used only computational primitive operations and for this reason RC5 algorithm should be appropriate for hardware or software [32]. Akihiro Shimizu and Shoji Miyaguchi (1988) presented a new block cipher algorithm for secure communications and store data called FEAL. FEAL is notation of Fast Data Encipherment Algorithm with block size 64-bit and 64-bit key length. FEAL similar to DES in protected data and it is suitable for both software and hardware implementations as DES [33].

3.2.2 Substitution-Permutation Networks (SPN): Introduction

Substitution- permutation network is another structures in Iterated product ciphers. Substitution- permutation network first introduced by Feistel et al (1975) refert to as SPN. SPN is series of mathematical operations used in block cipher. Substitution- permutation network consisting of a sequence of rounds of substitutions called S-boxes and connected by bit position permutations or transpositions [34] [35].

3.2.2.1. Advanced Encryption Standard (AES)

AES is the most widely used symmetric cipher. In 1997 call for AES by NIST, AES block cipher with 128-bit block size and include three key lengths must have supported 128, 192 and 256 bit. AES block cipher is efficiency in software and hardware, several industry and commercial systems include AES such as Internet security standard IPsec, IEEE 802.1, SSH (secure shell), etc. [36].In October 2, 2000 Rijndael method was selected as the AES algorithm, Jamil, T. (2004) Presented paper about a new advanced encryption standard (AES) called Rijndael algorithm approved by NIST. The Rijndael algorithm processes blocks of size 128,192 or 256 bits and supports symmetric keys of size 128,192 or 256 bits and note that Rijndael algorithm supporting larger key size than DES (Data Encryption Standard) supports. The Rijndael algorithm consists of three steps initial round called AddRoundKey, Standard Round consists of four transformations: Sub Byte, Shift Row, Mix Column and AddRoundKey, and the final Round also consists of Sub Byte, Shift Row and AddRoundKey but not including the Mix Column transformation. In overall performance, based onspeed of encryption/decryption processand key set-up time. This algorithm can apply in several applications such as smart cards and other applications which needed to storing and protecting sensitive information from unauthorized access [37]. Hanem et al. (2012) presented a new approach by modified S-boxes and key expansion procedure in advanced encryption standard called Modified Rijndael Algorithm (MRA) where designing small s-boxes defined over GF(2^4) rather than GF(2^8). the modified Rijndael algorithm achieve Confusion, diffusion and high security. From the performance evaluation of modified Rijndael algorithm prove that MRA is more suitable for the applications that require high security [38].Iqtadar et al. (2010)present a new encryption method based on a new S8 S-boxes to construct

ISSN 2278-7763

40320^{40320} secret keys. The new approach more secure for systems where consists of two parties to achieve secure communication channel, the exchange of secret message utilizes n^{40320} key options and the originator of the communication session require to change key with each message of length 16 for this a new encryption method gives more secure systems because if intruders attempt to break the code for these system needed to checks all n^{40320} keys or observes the alphabet frequencyof ciphering message. The new encryption method provides secure complexity as AES (Advanced Encryption Standard) [39].

3.2.2.1. SPN: Literature survey

There are several substitution-permutation networks block cipher methods proposed by researchers. In this section we will offer some of this methods and give short overview about each method.Kazys et al. (2015) presented a new approach for designing key-dependent S-boxes and inverse S-boxes generation algorithm for block cipher Systems where changing only one bit of key to generate key dependent S-boxes. S-boxes it is considered the main strength of the algorithm because it is a nonlinear transformation that provides confusion of bits, S-boxes achieves secure cipher against linear and differential cryptanalysis. The main characteristic of this algorithm it is that the change of secret key gives huge number of S-boxes [40].Hongjun et al. (2014) presented a new block cipher algorithm for authenticated encryption called AEGIS. AEGIS used to protect data and network packets. The new algorithm achieves speed 0.7 clock cycles/bytes for 4046 byte messages. AEGIS 128 uses five round function of AES and AES-256 uses six round function [41]. Jian Guo et al. (2011) presented paper about a new block cipher algorithm called LED algorithm. This algorithm aims to achieves and keep performance profile for software implementation and also LED block cipher dedicated to build-in hardware implementation [42].Daesung et al. (2003) presented papers offers a new encryption algorithm for block cipher called ARIA. ARIA processes data block of size 128-bits and based on substitution-permutation network structure of iterated product ciphers. ARIA uses only basic operation where use s-boxes the same as uses in the Rijndael algorithm as well as XOR operation so that it is efficient implementations for various environments (suitable for different platforms) [43].Joan et al. (1997) presented a new encryption algorithm for block cipher systems called SQUARE. A new algorithm based on substitution-permutation cipher and processes 128-bit block size and supported 128-bit key length. SQUARE block cipher algorithm designed against linear and differential attacks.SQUARE apply in several sensitive applications where it is efficient hardware implementations and has high parallelism [44].

There are several methods combine SPN and Feistel Cipher structure from this method Takeshi et al. (2002)presented a new encryption algorithm for symmetric block cipher called SC2000. The new block cipher based on both feistel and substitution-permutation cipher. SC2000 block cipher take 128-bit plain text and gives 128-bits cipher text with key length of 128-bit, 192-bit and 256-bit. The new SC2000 Symmetric block cipher algorithm provides

ISSN 2278-7763

high speed for both software and hardware implementations for different platforms and achieves high level of ciphering security [45]. Eli Biham et al. (1998) presented paper offers a new algorithm for block cipher to satisfying Advanced encryption standard (AES) requirements called Serpent. Serpent supported block size of 128-bit and 256-bit key length. The new algorithm is a very efficient implementations and high secure against all types of attack [46].

3.2.3 Unbalanced Feistel cipher: Literature survey

Generalized Unbalanced Feistel Network (GUFN) suggested by Schneier et al (1996) comparable to conventional feistel cipher, Unbalanced feistel cipher include a sequence of rounds in which the block is divided into two parts not equal in size. this change on feistel cipher has interesting implications for designing ciphers secure against linear and differential attacks[47]. Several block ciphers have been constructed based on Unbalanced Feistel Network whereTaizoShirai et al. (2007) presented a new encryption algorithm for block cipher systems called CLEFIA. The new algorithm based on unbalanced Feistel cipher and compatible with AES. CLEFIA has 128-bit input block and 128, 192, 256-bits key length. CLEFIA block cipher algorithm provides highly efficient implementations in both hardware and software, and also achieves high security against linear and differential Attacks [48]. Deuki Hong et al. (2006) presented a new encryption method for symmetric block cipher based on Generalized Unbalanced Feistel Network called HIGHT used for low resources devices and processes data block of size 64-bits and supported key length of size 128-bit. From security analysis prove that the new algorithm HIGHT block cipher has enough security for sensitive information against attacks [49]. Matt Blaze and Bruce Schneier (1995) presented a new block cipher based on unbalanced Feistel cipher in which each round of the cipher modifies only 16 bits for a function. MacGuffin similar to DES encryption algorithm in many characteristics as block size, application domain, performance and implementation structure. the block cipher includes 32-round and supported 64-bits block size and 128-bit size of key[50].in addition to above algorithm which based on unbalanced feistel cipher, there is many proposed methods based on this structure such as SMS4 cipher, Skipjack etc.

4. CONCLUSION

This Paper gives a short overview on cryptographic block cipher methods according to categories in cryptography. we give a study of the encryption algorithms proposed in this field according to classification it in cryptography such as DES, BLOWFISH, TWOFISH, etc. classified in Feistel Network, AES, AEGIS, ARIA, etc. classified in substitution-permutation networks and CLEFIA, HIGHT, MacGuffin, etc. classified in Generalized Unbalanced Feistel Network (GUFN).

ISSN 2278-7763

Where conclude that the classification of cryptographic Symmetric block cipher algorithms can be

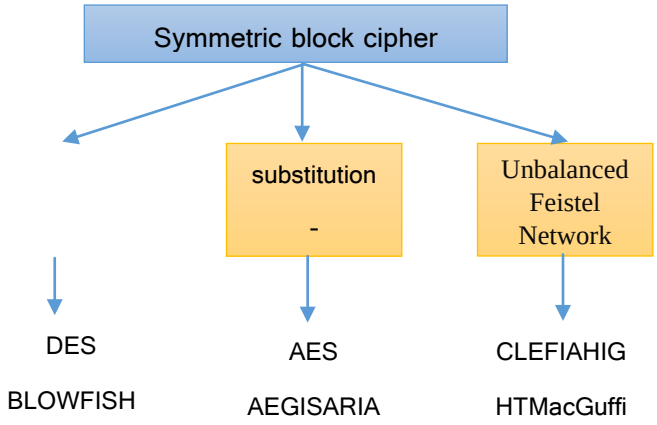

Fig3: Symmetric key block cipher classification

Among those categories the Generalized Unbalanced Feistel Network that is similar to conventional Feistel Network. Unbalanced Feistel Cipher split the block into two halves not equal in size. This change in design of Feistel cipher will be more efficient and more secure against linear and differential attacks.

REFERENCES

[1] Neelima Saini &Sunita Mandal, "Review paper on cryptography", International Journal of Research (IJR), e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015

[2] Douglas R. Stinson, Chapman and Hall/CRC," Cryptography: theory and practice ,"thirdedition (Discrete Mathematics and Its Applications),2005

[3] Coron, J.-S, "What is cryptography?", Security & Privacy, IEEE (Volume:4, Issue: 1), pp. 70- 73, 2006

[4] William stalling, "Cryptography and Network Security", 2011

[5] Ali M Alshahrani and Prof. Stuart Walker, "New Approach in Symmetric Block Cipher Security Using a New Cubical Technique", International Journal of Computer Science & Information Technology (IJCSIT) Vol 7, No 1, February 2015

[6] [illegible]s, Helmut Knebl, "Symmetric-Key Encryption", Springer Berlin Heidelberg, Introduction to Cryptography, Information Security and Cryptography, pp. 11-31, 2007

[7] Thomas W. Cusick and PantelimonStanica, "Cryptographic Boolean Functions and Applications", Academic Press, 2009

[8] E Surya, C.Diviya, "A Survey on Symmetric Key Encryption Algorithms", International Journal of Computer Science & Communication Networks, Vol 2(4), 475-477, 2012

[9] Lars R. Knudsen, "Block Ciphers -A Survey", Springer Berlin Heidelberg, State of the Art in Applied Cryptography, Lecture Notes in Computer Science Volume 1528, 1998, pp. 18-48, 1998

[10] C. Paar and Pelzl, Jan, "Understanding Cryptography, A textbook for students and Practitioners",Copyright Springer-Verlag , pp. 125

[11] Eli Biham, "On modes of operation", Fast Software Encryption, Lecture Notes in Computer Science Volume 809, pp. 116-120, 1994

[12] John Black and Phillip Rogaway, "A Block-Cipher Mode of Operation for Parallelizable Message Authentication", Springer Berlin Heidelberg, Advances in Cryptology — EUROCRYPT 2002, Lecture Notes in Computer Science Vol. 2332, pp. 384-397, 2002

[13] P. Rogaway, MihirBellare, John Black, "OCB: A block-cipher mode of operation for efficient authenticated

encryption",ACM Transactions on Information and System Security (TISSEC), Vol. 6, Issue 3,pp. 365-403, August 2003

[14] M Bellare, P Rogaway, D Wagner, "The EAX Mode of Operation", Springer Berlin Heidelberg, Fast Software Encryption, Lecture Notes in Computer Science Volume 3017, pp 389-407,2004

[15] Morris J. Dwork, "SP 800-38C. Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality", National Institute of Standards & Technology Gaithersburg, MD, United States ©2004.

[16] T. Kohno, J. Viega, D. Whiting, "CWC: A High-Performance Conventional Authenticated Encryption Mode", Springer Berlin Heidelberg, Fast Software Encryption, Lecture Notes in Computer Science Vol. 3017, pp. 408-426, 2004

[17] Shai Halevi and Phillip Rogaway, "A Parallelizable Enciphering Mode",Springer Berlin Heidelberg, Topics in Cryptology – CT-RSA 2004, Lecture Notes in Computer Science Vol. 2964, pp. 292-304, 2004

[18] David A. McGrew, John Viega, "The Security and Performance of the Galois/Counter Mode (GCM) of Operation",Springer Berlin Heidelberg, Progress in Cryptology - INDOCRYPT 2004, Lecture Notes in Computer Science Volume 3348, pp. 343-355, 2005

[19] Tetsu Iwata, "New Blockcipher Modes of Operation with Beyond the Birthday Bound Security", Springer Berlin Heidelberg, Fast Software Encryption, Lecture Notes in Computer Science Volume 4047, pp. 310-327, 2006

[20] Charanjit S. Jutla, "Encryption Modes with Almost Free Message Integrity", Springer-Verlag, Vol. 21, Issue 4, pp. 547-578, October 2008.

[21] MJO Saarinen, "SGCM: The Sophie Germain Counter Mode", IACR Cryptology ePrint Archive, 2011.

[22] C. E. Shannon, "Communication Theory of Secrecy Systems*", Bell System Technical Journal, Vol. 28, Issue 4, pp. 656–715, October 1949

[23] Kaisa Nyberg, "Generalized Feistel networks ", Springer Berlin Heidelberg, Advances in Cryptology — ASIACRYPT '96, Lecture Notes in Computer Science Volume 1163, pp. 91-104, 1996

[24] Lars R. Knudsen, "Practically secure Feistel ciphers", Springer Berlin Heidelberg, Fast Software Encryption, Lecture Notes in Computer Science Volume 809, pp. 211-221, 1994

[25] Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 2, December 2011.

[26] Zibideh, W.Y.; Matalgah, Mustafa M. "Modified DES encryption algorithm with improved BER performance in wireless communication," Radio and Wireless Symposium (RWS), 2011 IEEE, pp.219-222, Jan. 2011

[27] Seung-Jo Han; Heang-Soo Oh; Jongan Park, "The improved data encryption standard (DES) algorithm", Spread Spectrum Techniques and Applications Proceedings, IEEE 4th International Symposium on (Volume:3),1996.

[28] Xiao-Jun Tong; Zhu Wang; Yang Liu; Miao Zhang; Lianjie Xu, "A novel compound chaotic block cipher for wireless sensor networks," communications in Nonlinear Science and Numerical Simulation vol.22. Issues.1-3, May 2015, pages 120-133

[29] Rashmi; Chawla, Vicky; Nagpal, Rajni Sehgal Renuka," The RC7 Encryption Algorithm" International Journal of

Security & Its Applications. 2015, Vol. 9 Issue 5, p55-59. 5p.

[30] Bruce Schneier," Description of a new variable-length key, 64-bit block cipher (Blowfish)", Springer Berlin Heidelberg, Fast Software Encryption, Vol 809 of the series Lecture Notes in Computer Science pp 191-204, 2005

[31] B Schneier, J Kelsey, D Whiting, D Wagne, Chris Hall, Niels Ferguson, "Twofish: A 128-bit block cipher" - NIST AES 1998 - repo.hackerzvoice.net

[32] Ronald L. Rivest "The RC5 encryption algorithm", Springer Berlin Heidelberg, Fast Software Encryption, Lecture Notes in Computer Science Volume 1008, 1995, pp. 86-96

[33] Akihiro Shimizu, Shoji Miyaguchi "Fast Data Encipherment Algorithm FEAL" Springer Berlin Heidelberg, Advances in Cryptology — EUROCRYPT' 87, Lecture Notes in Computer Science Volume 304, 1988, pp. 267-278

[34] Howard M. Heys, Stafford E. Tavares,"Substitution-permutation networks resistant to differential and linear cryptanalysis", Journal of Cryptology, March 1996, Volume 9, Issue 1, pp. 1-19

[35] H. Feistel, W. A. Notz, and J. L. Smith. Some cryptographic techniques for machine-to-machine datacommunications. Proceedings of the IEEE, Vol.63 (Issue 11): pp.1545–1554, 1975

[36] Paar, Christof, Pelzl, Jan, "The Advanced Encryption Standard (AES)" Understanding Cryptography, A textbook for students and Practitioners", Copyright Springer-Verlag, Pages 87-121

[37] Jamil, T. "The Rijndael algorithm" Potentials, IEEE (Volume:23, Issue: 2) pp. 36 – 38, 2004

[38] Hanem M. El-Sheikh; Omayma A. El-Mohsen; TalaatElgarf; AbdelhalimZekry, "A New Approach for Designing Key-Dependent S-Box Defined over GF (2^4) in AES "International Journal of Computer Theory and Engineering Vol. 4, No. 2, April 2012.

[39] Iqtadar Hussain; Tariq Shah; Hasan Mahmood," A New Algorithm to Construct Secure Keys for AES "Int. J. Contemp. Math. Sciences, Vol. 5, 2010, no. 26, 1263 – 1270

[40] Kazys KAZLAUSKAS; GytisVaicekauskas; Robertas SMALIUKAS; "An Algorithm for Key-Dependent S-Box Generation in Block Cipher System "INFORMATICA, 2015, Vol. 26, No. 1, 51–65.

[41] Hongjun Wu; Bart Preneel, "AEGIS: A Fast Authenticated Encryption Algorithm" Springer Berlin Heidelberg, Selected Areas in Cryptography -- SAC 2013, Lecture Notes in Computer Science Volume 8282, 2014, pp. 185-201

[42] Jian Guo; Thomas Peyrin; Axel Poschmann; Matt Robshaw, "The LED block cipher, "Cryptographic Hardware and Embedded Systems – CHES 2011, Lecture Notes in Computer Science Volume 6917, 2011, pp 326-341

[43] Daesung Kwon, Jaesung Kim, Sangwoo Park, Soo Hak Sung, YaekwonSohn, Jung Hwan Song, YongjinYeom, E-Joong Yoon, Sangjin Lee, Jaewon Lee, Seongtaek Chee, Daewan Han, Jin Hong, "New Block Cipher: ARIA," Springer Berlin Heidelberg, Information Security and Cryptology - ICISC 2003, Lecture Notes in Computer Science Volume 2971, 2004, pp 432-445

[44] Joan Daemen, Lars Knudsen and Vincent Rijmen, "The block cipher Square" Springer Berlin Heidelberg, Fast Software Encryption Lecture Notes in Computer Science Volume 1267, 1997, pp.149-165

ISSN 2278-7763

[45] Takeshi Shimoyama, Hitoshi Yanami, Kazuhiro Yokoyama, Masahiko Takenaka, Kouichi Itoh, Jun Yajima, Naoya Torii, Hidema Tanaka, "The Block Cipher SC2000", Springer Berlin Heidelberg, Fast Software Encryption, Lecture Notes in Computer Science Volume 2355, 2002, pp. 312-327

[46] Eli Biham, Ross Anderson, Lars Knudsen, "Serpent: A New Block Cipher Proposal ", Springer Berlin Heidelberg, Fast Software Encryption Volume 1372 of the series Lecture Notes in Computer Science pp 222-238. 1998

[47] Bruce Schneier, John Kelsey, "Unbalanced Feistel networks and block cipher design", Springer Berlin Heidelberg, Fast Software Encryption, Lecture Notes in Computer Science Volume 1039, pp. 121-144, 1996

[48] TaizoShirai, KyojiShibutani, Toru Akishita, Shiho Moriai, Tetsu Iwata, "The 128-Bit Blockcipher CLEFIA" Springer Berlin Heidelberg, Fast Software Encryption, Lecture Notes in Computer Science Volume 4593, 2007, pp. 181-195

[49] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim,Sangjin Lee, Bon-Seok Koo,Changhoon Lee, Donghoon Chang, Jesang Lee, KitaeJeong, Hyun Kim, Jongsung Kim,Seongtaek Chee. "HIGHT: A New Block Cipher Suitable for Low-Resource Device",Springer Berlin Heidelberg, Cryptographic Hardware and Embedded Systems - CHES 2006, Volume 4249 of the series Lecture Notes in Computer Science pp 46-59

[50] Matt Blaze, Bruce Schneier, "The MacGuffin block cipher algorithm", Springer Berlin Heidelberg, Fast Software Encryption, Lecture Notes in Computer Science Volume 1008, pp. 97-110,1995

