High Lightweight Encryption Standard (HLES) as an Improvement of 512-Bit AES for Secure Multimedia

GUESMIA Seyf Eddine

Department of Computer Science,
University of M'sila
M'sila, Algeria

ASSAS Ouarda*

Department of Computer Science,
Laboratory Pure and Applied
Mathematics (LPAM)
University of M'sila
M'sila, Algeria

BOUDERAH Brahim

Department of Computer Science,
Laboratory Pure and Applied
Mathematics (LPAM)
University of M'sila
M'sila, Algeria

Abstract—In today's scenario, people share information to another people frequently using network. Due to this, more amount of information are so much private but some are less private. Therefore, the attackers or the hackers take the advantage and start attempting to steal the information since 2001. the symmetric encryption algorithm called 512-bit AES provides high level of security, but it's almost be impossible to be used in multimedia transmissions and mobile systems because of the need for more design area that effect in the use of large memory space in each round and the big encryption time that it takes. This paper presents an improvement of 512-bit AES algorithm with efficient utilization of resources such as processor and memory space. The proposed approach resists the linear and differential encrypt analysis and provides high security level using a 512-bit size of key block and data block and ameliorates the performance by minimizing the use of memory space and time encryption to be able to work in specific characteristics of resource-limited systems. The experimental results on several data (text, image, sound, video) show that the used memory space is reduced to quarter, and the encryption time is reduced almost to the half. Therefore, the adopted method is very effective for encryption of multimedia data.

Keywords—Advanced Encryption Standard (AES); Encryption; multimedia data; security; resource-limited systems

I. INTRODUCTION

Cryptology is the mathematical science of secret writing. It is made up of two halves: cryptography and cryptanalysis. Cryptography consists of the techniques for creating of secret writing. it uses mathematics to encrypt and decrypt data. Cryptanalysis encompasses the techniques of breaking that secret writing. itis the study of encrypted information in order to discover secret, Cryptanalysts are also called pirates. Over the past 2,500 years, cryptology has developed numerous types of systems to hide messages and subsequently a rich vocabulary in which to describe them. Cryptography consists of two parts: Symmetric Key Encryption and Public Key Encryption.

In Symmetric Key Encryption, both the sender and the receiver share the same key used for both encryption and decryption of the data. In fact, the two keys may be identical or trivially related.

In Public Key Encryption, two different keys related mathematically are used. Public key encryption encrypts data using the recipient's public key, and it cannot be decrypted without using a matching private key, and one key cannot be used in the place of the other [1].

The focus of this paper is stationed in the field of Symmetric Key Encryption. The improved AES algorithm that use 512 bit of key and data block provides high level of security, because of the use of key size larger by four times than the original 128-bit AES key [2]. However, it has a deficiency in performance, the encryption process become heavy when it comes to the modern communicating world that depends on the resource-limited systems and real-time operations

The main objective of this work is to design an alternative algorithm that keeps the level of security that the 512-bit AES provides, and minimizes the cost of memory and encryption time that it takes. The rest of the paper are details explain the proposed work as follow: Section 2 speaks about the original AES algorithm with more details and a given algorithm called 512-bit AES that was appeared to provide more security. Section 3 talks in details about the proposed algorithm that is given as an alternative to the one that called "512-bit AES" for improving the performance level, explaining its transformations methods including the general architecture and key expansion. In section 4, we talk about the tests that we have done and the results that prove the amelioration of the performance level. Finally, section 5 concludes the paper with a general thought about HLES algorithm.

II. RELATED WORK

The proliferation of digital communications, multimedia and the transition of social interactions into the cyberspace have raised new concerns in terms of security, trust and performance. The selection of a suitable crypto-algorithm will dynamically affect the lifespan and performance of a device in terms of battery-life, hardware memory, computation latency and communication bandwidth. To select a suitable cryptographic algorithm for an application or an environment, the understandings of both the algorithmic requirements in terms of hardware and the specifications of the development platform intended has to be established.[3].The National Institute of Standards and Technology (NIST) established a powerful encryption algorithm for symmetric encryption procedures called Advanced Encryption Standard. AES is a Federal Information Processing Standard (FIPS) that has three variable

key lengths but block length is fixed to 128 bits. The three key sizes of AES are 128, 192 and 256 bits. [4]. Their number of possible keys is 2127, 2191 and 2255 respectively. [5]. AES was designed to have very strong resistance against the differential cryptanalysis and linear cryptanalysis attacks since it used Wide Trail Strategy in its design. [6]. The United States government organizations has approved for the AES to be used to protect sensitive, unclassified information. It was also widely adopted both commercially and globally. [5]. To enhance the reliability of the algorithm against the brute force attack and provide more security,A new algorithm structure appeared in 2011 that is similar to the original AES algorithm, but having slight difference is that the plaintext size and key size use input of 512 bit instead of 128 bit. It consist of the same four major operations of the original AES performed during each round: byte substitution, shifting rows, mixing columns and finally adding the round key. However, they are designed to be bigger than the original AES operations by four times to be able to occupy the 512 block and key size. this version of AES can be used when higher level of security throughput are required, because more security comes from using larger key size, and more throughput comes from using four times larger block size that the block size used in the original AES. [2]. However, in the modern communicating world with all its ways including the wireless mobile systems and videos that generally process a large amount of data and require real-time operations, there is limited processing power, memory and bandwidth, and is rarely able to provide such security level and handle the heavy encryption-processing load in same time. Real Time Applications (RTA) are application programs that function within a specific timescale. Voice over IP (VoIP) and video conferences are examples of RTA. Transmitting such data via open networks is risky. However, any security must be lightweight and cause no delay. Recently, many algorithms have been created (RC4 (Rivest Cypher 4), RC5 (Rivest Cypher 5), RSA (Rivest Shami Adleman) …), but very few are viable with RTA. [7]. In addition, it is difficult to use encryption techniques directly in multimedia data because of the large volumes, and require real-time interactions. Therefore, there is a need of efficient and light encryption algorithm as an alternative, which can provide better security and performance. [8]. Based on the state of multimedia encryption, can observe that:

- For complete and provable security of the video data for example, the entire video needs to be encrypted. However, a naive encryption of the complete video stream is computationally slow.

- To solve the problem of speed, there is a need of finding solutions to the naive encryption.

- The traditional naive encryption methods use conventional AES algorithm. There is a need of modification in the algorithm to reduce the time required for encryption and increase the security level.

- The encryption algorithm should not be susceptible to attacks like known plaintext attack and cipher-text-only attack. Computational efficiency should not come at the cost of security.

III. PROPOSED APPROACH

The aim of this paper is to present a new light algorithm called High Light weight Encryption Standard (HLES) that can be used when higher level of security throughput are required, and processing power, memory space and bandwidth are limited (case of multimedia transmissions and mobile systems).

The HLES algorithm uses a key size of 512 bit and data block size of 512 bit. Both of key and data block are divided to 4 blocks of 128 bit for each. Each set of those four 128-bit blocks will be encrypted using an encryption functions that produce a set of four 128-bits encrypted blocks using four 128-bits encryption keys. The encryption process use each one of the four key parts to encrypt the four data block parts respectively but not in same time so that the memory consummation can be minimized. The four encrypted parts are not independents because each part needs the previous one to continue the encryption process (except the first one because it has no previous part).

The proposed algorithm called HLES has four main different transformations. The first transformation is the byte substitution that substitutes the value of 16 bytes and this is achieved via using parallel S-Boxes.

The second transformation is the (SH-Z) function that translate bytes (data block and key block) to bit-stream block and calculate the number of zeros exist in the bit-stream key block, then shift the bit-stream data block to the left side as the calculated number of zeros, after that it retranslate the bit-stream block to bytes data block.

The third transformation is a normal XOR function applied with 128-bit key part and 128-bit data block part. The final transformation has the same role of the previous one (XOR function) but this one is applied with the current part and result of previous part.

A. Architecture

The placement of functions is designed and chosen carefully to guarantee a lower cost of computational resources and good performance. In addition, its architecture provides high level of security because of the 512-bit key length and a special coordination and synchronization between its functions. The encryption process and functions placements are shown as a flowchart in the figure (Fig.1).

- Bytes substitution :The 512 bits input plaintext is divided into four 128-bit parts. Each part is organized in array of 16 bytes that are substituted by values obtained from substitution boxes. The S-Box used in the proposed algorithm is the same one used in the AES algorithms in case there is no need to generate a new one because of its proven effectiveness. This is done to raise the security level according to diffusion-confusion Shannon's principles for cryptographic algorithm design [9]. The S-Box is shown in the figure (Fig.2).
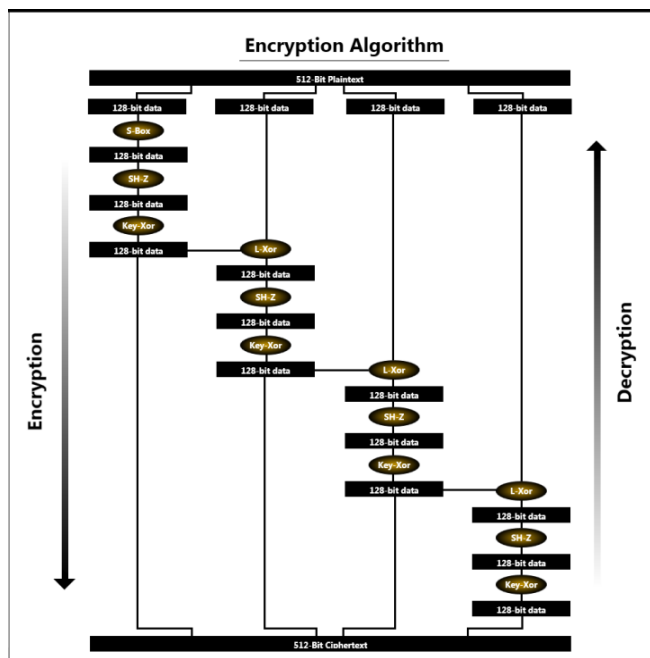
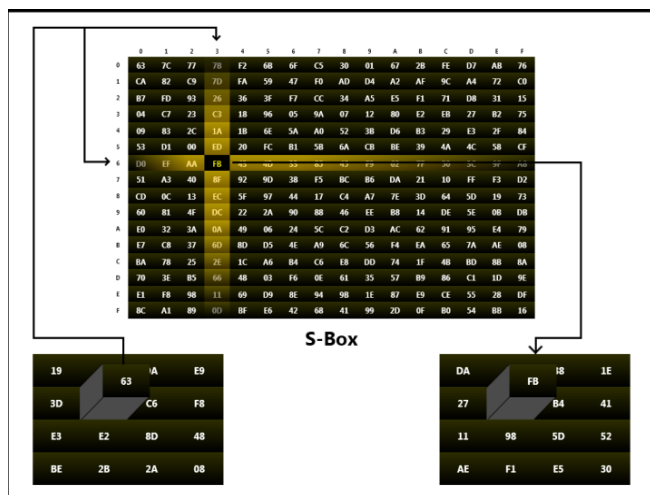Fig. 1.   HLES General Architecture
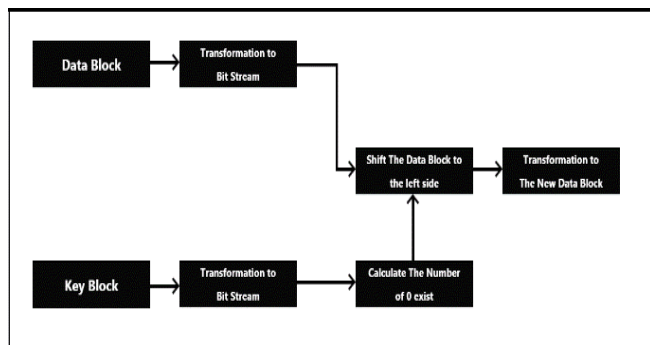

Fig. 2.   Byte Substitution

Fig. 3.   SH-Z Bit stream shift function

- SH-Z function: This function depends on the number of zeros exist in each 128-bit part of key applied in the block. First, two matrix of bytes (data block part and

key block part) are translated to bit-stream blocks. Second, number of zeros exist in the bit-stream block of key part is calculated. Then, bit-stream block of data is shifted to the left side as the calculated number of zeros. Finally, that bit-stream block of data is retranslated to a result matrix of bytes. The figure (Fig.3) explain the procedure.

- Key-Xor and L-Xor functions: Both functions are EXCLUSIVE-OR functions (called EXCLUSIVE DISJUNCTION functions in some references) the difference between them is the inputs that they use. Key-Xor function depends on the outcome of each process of HS-Z function and each 128-bit key part block to produce a part of cipher text, this function is applied on all the four block parts as shown in the flowchart of the HLES general architecture. L-Xor function depends on the previous outcome of the Key-Xor function and the current block part, it is applied on the last three block parts, because the first one has no previous outcome of HS-Z function.

B. Key expansion and rounds

The original AES uses a key whose length is 128, 192 or 256 bits. The cipher key is expanded to into 10, 12, or 14 round keys, respectively, using the Key Expansion Algorithm, where each round key is of 128 bits. This Key Expansion algorithm depends only on the cipher key, and is independent of the processed data. It can therefore be executed in dependently of the encryption / decryption phase. The round keys are the combination of transformations SubWord (RotWord(tmp)) and SubWord (tmp) and the use of the RCON value. The AES Key Expansion algorithm is described by the pseudo code in the Figure (Fig.4) (the pseudo code is written in terms of double words). [10].

Fig. 4.   Key expansion pseudo code

Through research and analysis of 128-bit AES key generation and extension mechanism, only if the attacker gets the wheel of the sub-keys, he can deduce all the sub keys by the AES key generation expansion mechanism. As we can find a new way which can generate sub keys from front to back quickly, but the reverse derivation of the keys causes difficulties. It can both increase the difficulty of brute force AES and can effectively prevent the weaknesses of a variety of AES key expansion attack, and will not affect the speed of its

current run. [11]. In HLES algorithm, the key is divided to four parts of 128-bit that are expanded to occupy 10 rounds. Therefore, the key expansion algorithm that the original 128-bit AES use is enough since it was and still until now one of the most strong key expansion algorithms against the related key attacks. [12].

IV. RESULTS AND EVALUATION

In order to compare between the three encryption algorithms (128-bit AES, 512-bit AES and HLES), there designs were coded in same operating system (Microsoft Windows 7), same programming platform (Visual Studio Platform), same environment (WPF environment) using same programming language, which is C# language. The used operation mode is the ECB mode (Electronic CodeBook), which is the simplest one. We used five data blocks of different memory capacities to be encrypted, (text file, JPG image, PNG image, MP3 sound, MP4 video). First one is text file of 5.8 Kbytes, second one is JPG image of 25 Kbytes, third one is PNG image of 59 Kbytes, forth one is MP3 file of 105 Kbytes (sound file), and the last one is MP4 file of 219 Kbytes (video file), and we calculated there encryption time. The synthesis results are shown in the table (TABLE I):

TABLE I. COMPARISON OF THE THREE ALGORITHMS (128-BIT AES, 512-BIT AES, HLES)

	128-bit Algorithm	512-bit Algorithm	HLES Algorithm
TXT file (5810)	81	167	64
JPG file (25000)	280	566	228
PNG file (59000)	871	1352	577
MP3 file (105000)	1961	2314	1010
AVI file (219000)	4842	5389	2529

The results show that the proposed algorithm (HLES) encrypts the data spending time less than what the original 128-bit AES spend, and almost the half time that the 512-bit AES spend, and the difference is getting bigger in each time the data gets bigger. The figure (Fig.5) presents the encryption time for the three algorithms, 128-bit AES (in Red), 512-bit AES (in Green), HLES (in blue).

When it comes to the criteria of the memory space, there are two ways to effect an ideal comparison. The first one is to measure the memory space spent by all the functions of the encryption process, in this case, to encrypt one data block of 512-bit size, the 512-bit AES uses four functions that occupy together 2048 bits (512-bit x 4). While the area design of the proposed algorithm (HLES) allows to occupy only 1536-bits (128-bit x 3 x 4), which is less than the other one by 1/4. The second one is to measure the memory space spent by each function of the encryption process. In this case, we have to take in consideration the size of data block that each function consume at the same time for each algorithm. In 512-bit AES, all the functions work with 512-bit data block size. While in HLES algorithm there are functions that work with 128 bit

block size and functions that work with 256 bit block size (functions that need two 128 bit blocks to produce one 128 bit block), but generally HLES algorithm has no function that consume more than 256 bit.
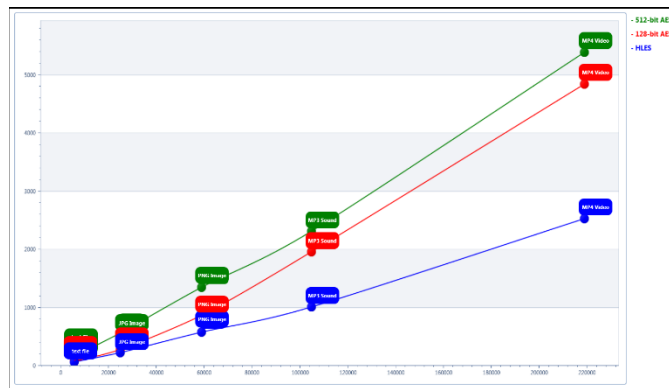

Fig. 5. Comparison of the three algorithms in encryption time using five kinds of files (text file, JPG image, PNG image, MP3 sound, MP4 video)

The proposed algorithm (HLES) uses memory space less than the other one that 512-bit AES uses, which makes it acceptable to be used in resource-limited systems.

V. CONCLUSION

In this work, we proposed a light symmetrical algorithm as an alternative to the 512-bit AES that provides high security level using a 512-bit size of key block and data block, and resisting the brute force attack with efficient utilization of resources such as processor and memory space. HLES ameliorates the performance by minimizing the consummation of memory and time encryption to be able to work in specific characteristics of resource-limited systems. The experiments show that the memory usage is minimized by one quarter of the one that the algorithm called 512 AES uses, and the encryption time is reduced almost to the half, which makes it near in performance to the original 128-bit AES. The future work will be focused on promoting operation speed of key expansion to ensure a good synchronization between key generating and encryption process. Moreover, all possible key attacks will be tested and examined.

REFERENCES

[1] C. Haldankar1, S. Kuwelkar2, "Implementation of AES and Blowfish Algorithm", International Journal of Research in Engineering and Technology (IJRET), Volum: 03 Special Issue: 03, May-2014, pp: 143-146.

[2] A. Moh'd, Y. Jararweh, L. Tawalbeh, "AES-512: 512-bit Advanced Encryption Standard design and evaluation", 7th International Conference on Information Assurance and Security (IAS), 2011, 5-8 December 2011, Melaka, Malaysia, pp: 292-297.

[3] J. H. Konga, L. Angb, K. P. Sengb, "a comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments", Journal of Network and Computer Applications 49 (2015), volum: 49, 14 October 2014, pp: 15-50.

[4] F. S. Hossain, L. Ali and N. Roy, "design and analysis of a high Performance AES Processor", 6th International Conference on Electrical and Computer Engineering (ICECE) 2010, 18-20 December 2010, Dhaka, Bangladesh, pp: 562-565.

[5] W. E. BURR, "Selecting the Advanced Encryption Standard", IEEE SECURITY & PRIVACY, ISSN: 1540-7993, IEEE , Volum: 1, Issue: 2, Mars-April 2003, pp: 43-52.

[6] J. Gui, L. Huang, H. Zhong, C. Chang and W. Yang, "An Improved AES S-BOX and Its Performance Analysis, International Journal of Innovative Computing", Information and Control (ICIC), Volume: 7, Number 5(A), May 2011, pp: 2291-2302.

[7] B.Subramanyan, V.M.Chabria, T.G.Sankar babu, "Image Incryption Based On AES Key Expansion", 2nd International Conference on Emerging Applications of Information Technology (EAIT), 2011, 19-20 February 2011, Kolkata, India, pp: 217-220.

[8] P. Dechmukh,V. Kolhe, "Modified AES Based Algorithm for MPEG Video Encryption", International Conference on Information Communication and Embedded Systems (ICICES), 2014, 27-28 February 2014, Chennai, India, pp: 1-5.

[9] DJ. E. Goumidi, F. Hachouf, "Modified confusion-diffusion based satellite image cipher using chaotic standard", logistic and sine maps, 2nd European Workshop on Visual Information Processing (EUVIP), 2010, 5-6 July 2010, Paris, France, pp: 204-209.

[10] J. J. Tay, M. M. Wong, I. Hijazin, "Compact and Low Power AES Block Cipher Using Lightweight Key Expansion Mechanism and Optimal Number of S-Boxes", IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), 2014, 1-4 December 2014, Kuching, Malaysia, pp: 108-114.

[11] D. R Grandh, V.Kamalakannan, R.Balamurugan, S.Tamilselvan, "FPGA Implementation of Enhanced Key Expansion Algorithm for Advanced Encryption Standard", International Conference on Contemporary Computing and Informatics (IC3I), 2014, 27-29 November 2014, Mysore, India, pp: 409-413.

[12] D. Chen, D. Qing, D. Wang, "AES Key Expansion Algorithm Based on 2D Logistic Mapping", 5th International Workshop on Chaos-fractals Theories and Applications (IWCFTA), 2012, 18-21 October 2012, Dalian, China, pp: 207-211.