A REVIEW ON HIGH SPEED ADVANCE ENCRYPTION STANDARD (AES)

Pushpinder Kaur, Preeti Gupta, Sanjiv Kumar
UIET, PU , Chandigarh, India

ABSTRACT - AES is one of the algorithms that are used for data security transmission. Using AES we can secure our data while sending from one person to other person. Our data can be in the form of text data, image data, video data, animated data etc. Need of AES is to stop the cyber-thief that could stole your keystrokes and access your passwords, credit card numbers and important information. AES is a specification for the encryption of electronic data. Established by the National Institute of Standards and Technology (NIST) in 2001, it has been adopted by the US government and other nations to protect confidential data and information. Pipeline algorithm is one of the algorithms which used to increase the speed and operational frequency. AES can be implemented on FPGA to improve security and to validate the results. Many authors are trying to achieve max frequency and low slices due to which speed will be increased to secure data.

Keywords - Advance Encryption Standard, Cryptography, Field Programmable Gate Array, Substitution box

I. INTRODUCTION

Cryptography is a method of transmitting and storing data so that only that person can read the information which is authenticated. Cryptography is used for secret data transfer that is in the form of symmetric and asymmetric key. In symmetric there is only one type of key i.e. common key for both encryption and decryption called as secret key cryptography. In Asymmetric key cryptography uses two types of keys for encryption and decryption. It uses public key for encryption and private key for decryption. This is called public key cryptography. Cryptography AES algorithm is Established by the National Institute of Standards and Technology (NIST) in 2001, it has been adopted by the US govt. and other countries to protect confidential data and information [1]. The criteria characterized by NIST for choosing AES fall into three regions i.e. Security, Cost and Implementation. Hardware and software both implementations are done in AES. In AES they are processing data bits of 128 bits by using cipher key of length 128,192 or 256 bits [2]. Hardware implementation is used for better physical security and speed as compare to software implementation. High speed is also required for secure communication for one to other person. Fig 1: shows Some Symmetric key cryptographic algorithms.

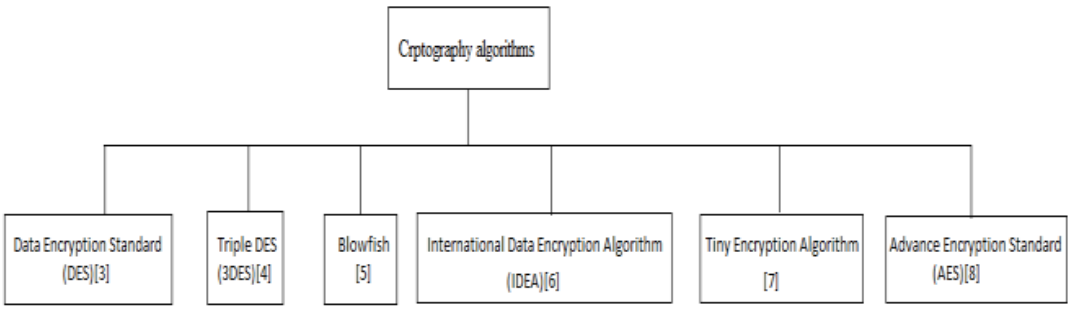

Fig 1: Types of cryptography algorithms

After analysis of these entire algorithm AES was selected as best depending upon security, cost and implementation by NIST. There are some attacks or flaws on AES that are Brute-Force attacks, Unauthorized access, Side channel effects, Complexity due to S-box, DPA attacks etc. and can be improved by pipeline algorithm, Cryptography algorithm, Evolutionary algorithm etc. General assaults that were uncovered against concentrated rounds versions of Rijndael are Square Attack, Improved Square Attack, Impossible Differential Attack and Reversed Key Schedule Attack, however none of the assaults are possible in reality[9].

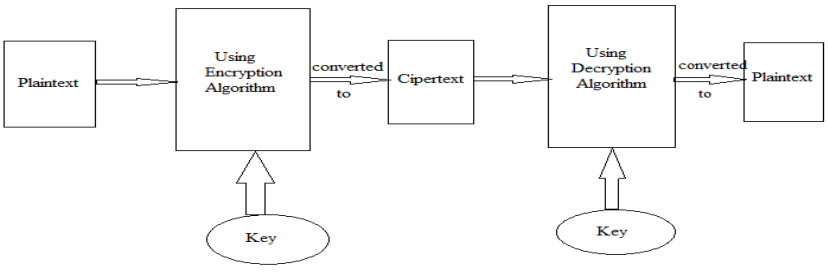

Fig 2: Basic AES Process

II. WORKING OF AES

Basic process of AES is that when we send some information from one person to other person that information in form of plain text and using key we encrypt that data called as cipher text while sending the information. The person who receives that information can decrypt cipher text to plain text using same secret key. Encryption algorithm consists of following steps:

A. Convert State array

Input given to the AES is in the form of text message and converts that message in the form of blocks. Then convert that block in the form of state array

B. Transformations and their inverse

a) Add Round Key: In the state array there are rows and columns. Each column represents the byte. XOR operation is done in each round of state array and round key which gives us new state array with Add Round Key, as shown in fig. 3.

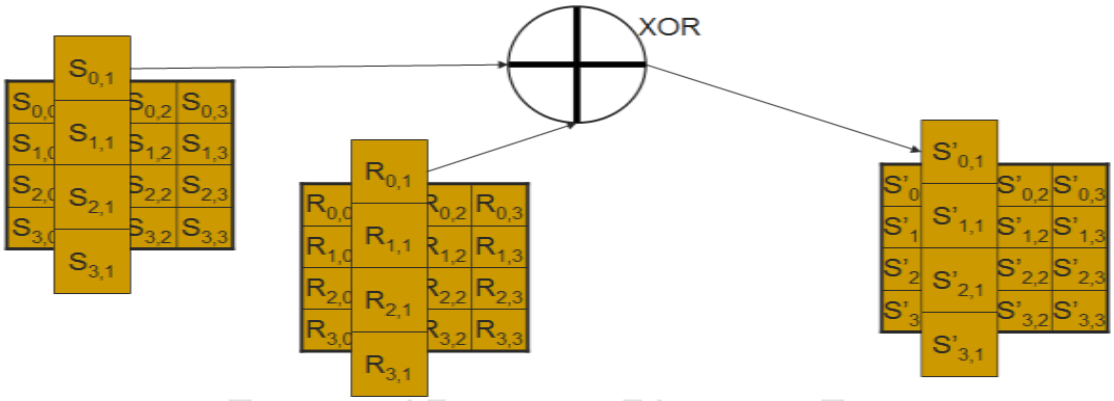

Fig 3: XOR of State Array

b) Sub-bytes: The S-box (Substitution box) [7] is non-liner substitution of AES. The Sub-Byte is a non-linear byte substitution process, utilizing a substitution table (S-box), which is composed by augmentation, shown in Fig. 4.

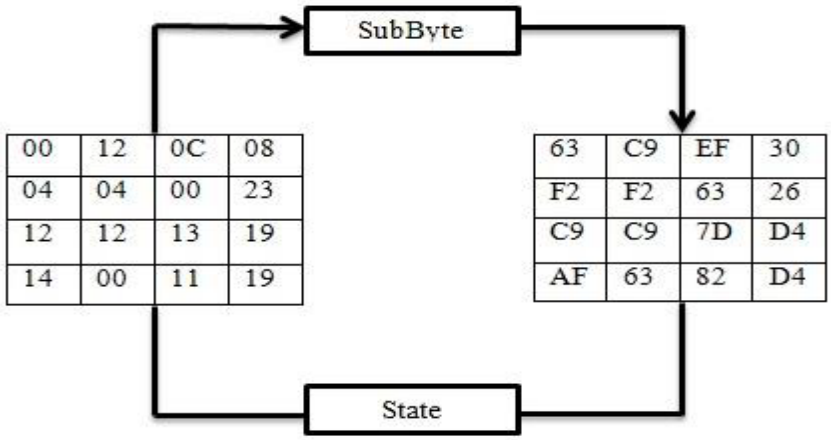

Fig 4: AES diagrams for Substitution step [1]

c) Shift Rows: State array rows are shifted cyclically. Fig. 5 below explains the shifting process. First row is not shifted by none byte. Second row is shifted by one byte; third row is shifted by two bytes and so on.

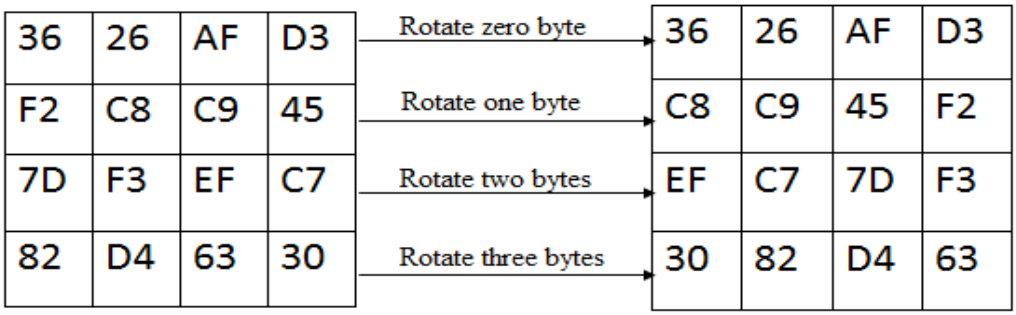

Fig 5: Shifting rows of AES

d) Mix columns: Fourth step after Shift Rows is Mix columns. Mix column is linear process where state matrix columns are independent on each other and new columns of state matrix are created by shuffling four bytes of each column, shown in fig.6.

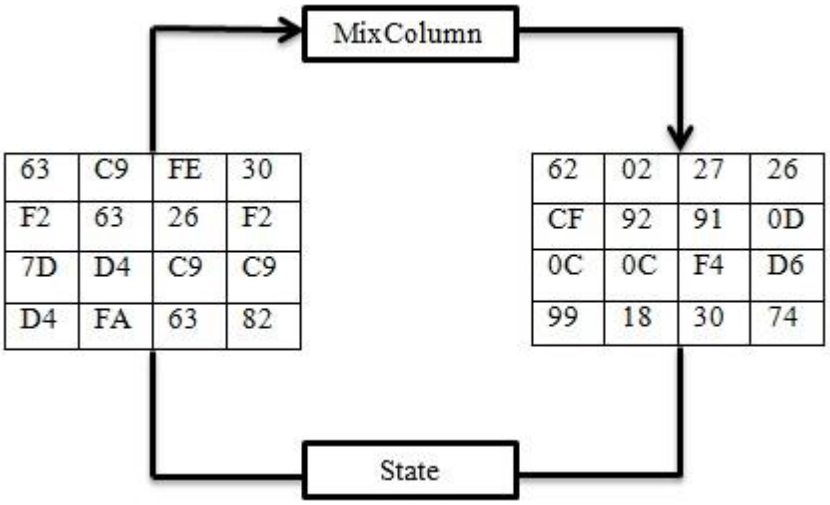

Fig 6: Mix columns of AES [1]

C. Key Expansion

Key expansion is to increase the security so that no one hack the key. Key Expansion is done so that in each round uses a new round key.

Decryption is just inverse of encryption. Decryption is used to convert the ciphertext to plaintext using decryption algorithm. Fig. 7 shows the whole process of AES algorithm.

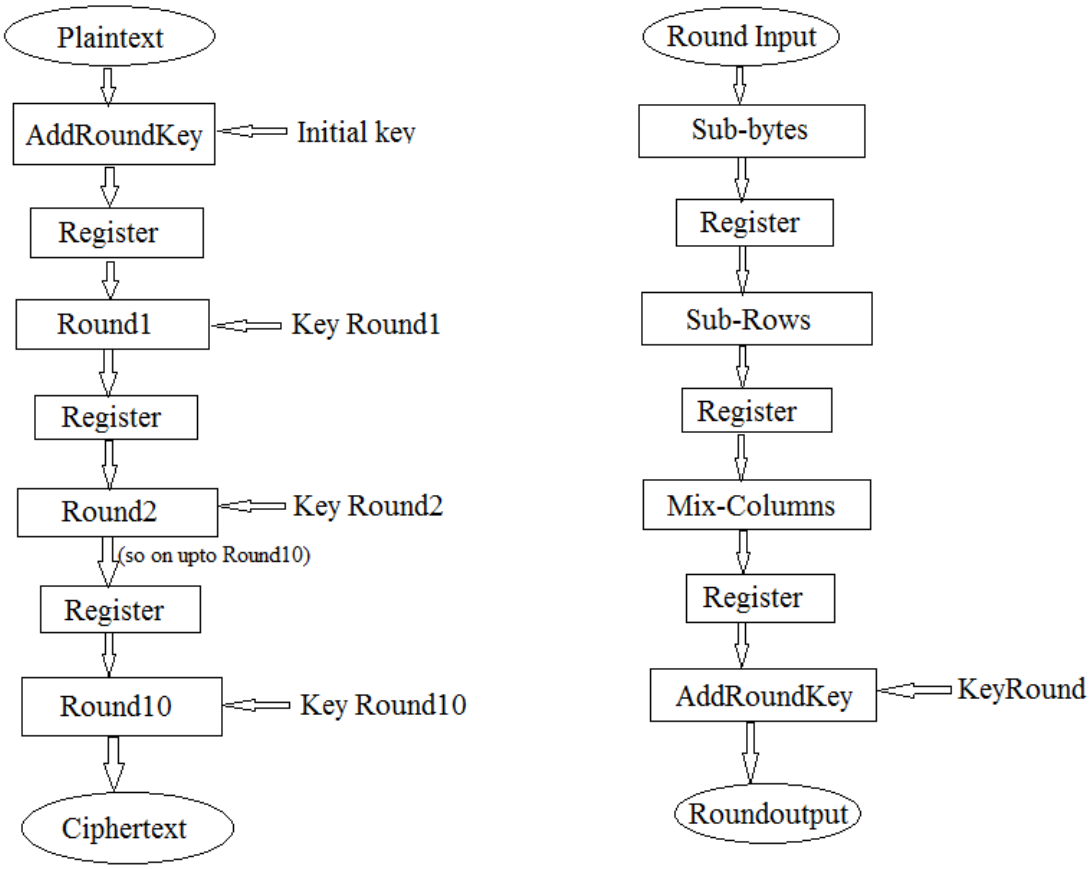

Fig 7: General AES block and rounds of AES [2]

III. LITERATURE REVIEW:

Mustafa.E.H et al describes that using standard symmetric encryption algorithm some attacks can be prevented. This paper still required some improvement for encryption of data and to prevent attacks [1]. The author Yu.W and S. Köse describes an implementation of modified lightweight in FPGA. AES algorithm such as mix columns, shift rows, substitution byte all are come in parallel manner. AES is more secure in hardware implementation and also have less cost and minimized hardware utilization [10]. The author proposed a false key based AES algorithm to prevent leakage of stored key from substitution box under CPA (correlation power analysis) attacks without significant power[11]. The authors Bri.S and Oukili.S describe the high speed for efficient AES implementation. After analysis conclude that it consumes low area and gives better throughput using pipelining technique [2]. For Unauthorized access speed of AES must be high and have strong cryptography. Authors S. Bri and S. Oukili used 5-stage pipeline design for maximum frequency and used to increase speed [12]. This paper explores the switching Capabilities of BRAM and by changing duty cycle of input clock. Work done by this author is by using pipeline design and saved area by 59.01% [13]. The non-pipelined plans [14–16] concentrated on the reduced plan and are more proficient when AES works in the input mode, where the new plaintext should be first included with the already encoded cipher text. The main outline choice is the quantity of pipelining stages in each figure round. In [17–21], different quantities of stages were investigated, prompting diverse throughput. The second outline choice is the usage of S-box in Sub-Bytes. The composite-field calculation based S-box accomplished littler territory contrasted with the LUT based usage in ASIC executions [22, 23]. For FPGA with four-input LUTs, the composite-field usage can likewise decrease zone. Nonetheless, for late FPGA with six-input LUTs, the circumstance is changed, and the LUT-based usage of S-box has littler region and lessened deferral. We will see the related exploratory outcomes in the accompanying area. In this way we pick the main answer for actualize S-box. It was specified in [19, 20, 21] that the LUT in the first arrangement constrains additionally parcelling of pipelining stages in each round of AES. This restriction is settled in the display paper by partitioning S-box into sub-boxes. J.-Y. Park *et al.* [24] chipped away at strategies for viable white-box cryptography. In this assaults are considerably more grounded then the discovery display. The fundamental confinement of this plan was switching of look into table which is quick and solid if there should arise an occurrence of the white box and considered for the future research. Gaspar et al. [25] chipped away at effective AES S-boxes execution for non-unstable FPGAS. They proposed a proficient strategy for the execution of AES byte substitution work (S-box). The proposed an answer which requires less space and is speedier than the one executing entire S-encloses the rationale region. The principle confinement of this plan was FPGA can't be utilized for the low battery purposes. Selimis et al. [26] chipped away at applying low power procedure in AES MixColumn or InvMixColumn transformation. They research the utilization of low power assets which expands the security needs and effectiveness. Along these lines, the information ways which are of no utilization for the framework are deactivated and increment the adaptability of the framework for the better outcomes. Watercourse et al. [27] took a shot at top notch picture encryption calculation in view of AES modification. They examined piece figure calculation surely understood AES as it is more secure. The fundamental constraint of this plan was the encryption/unscrambling time required was increasingly and the assaults on the encryption calculation can lessened the rounds. Goodwin et al. [28] worked on AES usage with expanded differential power investigation (DPA) obstruction and low overhead. They explore aside channel assault that presented to potential shortcomings for the specific power examination. In this way, they talked about enhanced quality against side channel assaults with insignificant extra equipment overhead. Berna et al. [29] presented control examination assault on an ASIC AES execution. They chipped away at side direct assault in which it isn't that simple to extricate the mystery data.

After studying different techniques pipelining is the good choice for better speed, throughput and efficiency. From Table I, we can conclude that using pipelining method we can achieve high throughput in which key expansion and other steps will be done in parallel processing. We can use composite field arithmetic, direct mapping from LUT or using combinational logic technique in Xilinx-14.7 while using the pipelining method. From all of above methods we prefer combinational logic method for small area and high speed. FPGA implementation will be done on vertex using Xilinx-14.7 (ISE design suite). Hardware implementation is important as there is no memory in hardware but data is stored in the form of low and high voltage do it is difficult to access data. So hardware implementations and pipelining will be done to achieve low area and increase speed of AES. Hardware implementation is done to validate the results.

Table I. Comparison

Author	Tech. used	Devices	Output Parameters			
			Slices	Throughput (Gbps)	Max-freq. (MHz)	Efficiency
Wang *et al.*[19]	GF-method	Virtex	5927(×2)	44.07	344.12	3.71
Yi Wang *et al.*[30]	Pipeline	Virtex XC6VLX240T	6784	28.7	283.2	4.2
Rahimunnisa *et al.* [31]	Pipeline	Virtex-6 XC6VLX75T	2597	59.59	450.045	22.94
Liu *et al.* [32]	Pipeline	Virtex-6 XC6VLX240T	3121	64.1	501	20.54
Sharma *et al.* [33]	Pipeline	Virtex-5 XC5VLX85	5759	68.12	532.19	11.82
Liu *et al.* [34]	Pipeline	Virtex-6 XC6VLX240T	3900	73.39	573.39	18.81
Wang and Ha [35]	Pipeline	Virtex-6 XC6VLX240T	5613	78.22	611.06	13.9
Bri.S and Oukili.S [2]	Pipeline	Virtex-6 XC6VLX240T	4830	79	617.627	16.36

REFERENCES

[1] Hameed, M. Emad, M. M. Ibrahim, and N. A. Manap, "Review on improvement of Advanced Encryption Standard (AES) algorithm based on time execution, differential cryptanalysis and level of security," Jour. of Telecom, Elect. and Comp. Engg. , vol. 10, no. 1, pp. 139-145, 2018.

[2] Brown, L.S. Bri, Oukili and Soufiane. 2017, "High speed efficient AES implementation," In Proceedings of the ISNCC conference in IEEE.

[3] S.P. Singh and R. Maini, "Comparison of data encryption algorithm," International Jour. of Comp. Sci. and Comm. vol. 2, no. 1, pp. 125-127, 2011.

[4] Barker, William C., and B.B. Elain, "SP 800-67 revision 1 recommendation for the Triple Data Encryption Algorithm (TDEA) block cipher," 2012.

[5] Nie, Tingyuan and T. Zhang. 2009, "A study of DES and blowfish encryption algorithm," In Proceedings of Tencon 2009-2009 IEEE Region 10 Conference, IEEE.

[6] Zimmermann, R. Curiger, A. Bonnenberg, H. Kaeslin, H. Felber, "A 177 Mb/s VLSI implementation of the international data encryption algorithm." IEEE Jour. of Solid State Circuits, pp. 303-307, 1994.

[7] Wheeler, J. David, and R. M. Needham,"TEA, a tiny encryption algorithm," in Intr. Workshop on Fast Soft. Encryp., " Springer, Berlin, Heidelberg, pp. 363-366, 1994.

[8] Zhang, Xinmiao, and K. K. Parhi. "High-speed VLSI architectures for the AES algorithm," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, pp. 957-967, 2004.

[9] O. S. Dhede and S. K. Shah. 2015, "A review: Hardware implementation of AES using minimal resources on FPGA", Inter. Conf. on Pervasive Comp., IEEE.

[10] M. James, D. S. Kumar. 2016, "An implementation of modified lightweight advance encryption standard in FPGA" Procedia Technology, Elsevier, vol. 25.

[11] Yu.W and S. Köse, "A lightweight masked AES implementation for securing IoT against CPA attacks" IEEE Trans. on circuits and systems-I: Regular papers, vol. 64, no. 11, Nov 2017.

[12] S. Bri and S. Oukili, "High speed efficient FPGA implementation of pipelined AES S-Box," High school of Technology, Moulay Islamil University Meknes, Morocco, 2016.

[13] Kundi, D. S., A. Aziz, N. Ikram, "A high performance ST-Box based unified AES encryption/decryption architecture on FPGA" , Microprocessors and Microsystems, pp. 37–46, 2016.

[14] Hussain, Ulfat, H. Jamal. 2012, "An efficient high throughput FPGA implementation of AES for multi-gigabit protocols,"In Proceedings of International Conf. Frontiers of Info. Tech., pp. 215–218.

[15] Rais, M.H., S.M. Qasim, "Efficient hardware realization of advanced encryption standard algorithm using Virtex-5 FPGA," Int. Jour. Comp. Sci. Netw. Secur., vol. 9, pp. 59–63, 2009.

[16] Rais, M.H., S.M. Qasim, "A novel FPGA implementation of AES-128 using reduced residue of prime numbers based S-Box," Int. Jour. Comp. Sci. Netw. Secur., vol. 9, pp. 305–309,2009.

[17] A. Hodjat, I. Verbauwhede. 2004, "A 21.54 Gbits/s fully pipelined AES processor on FPGA," In Proceedings of IEEE International Symp. Field Prog. Custom Comp. Machines, pp. 308–309.

[18] T. Good, M. Benaissa, "AES on FPGA from the fastest to the smallest," Cryptographic Hardware and Embedded Systems, ser. Lecture Notes in Computer Science, Springer, Berlin/ Heidelberg, pp. 427–440, 2005.

[19] Y Wang, Y. Ha, "FPGA-based 40.9-Gbits/s masked AES with area optimization for storage area network," IEEE Trans. Circuits Syst. II: Express Briefs, vol. 60, pp. 36–40, 2013.

[20] K.U. Järvinen, M.T. Tommiska, J.O. Skyttä. 2003, "A fully pipelined memoryless 17.8 Gbps AES-128 encryptor," In Proceedings of International Symp. Field Prog. Gate Arrays, ser. FPGA, New York, NY, USA, pp. 207–215.

[21] Reddy, S. K., R. Sakthivel, and P. Praneeth, "VLSI implementation of AES crypto processor for high throughput," Int. Jour. Adv. Eng. Sci. Tech., vol. 6, no.1, pp. 22–26, 2011.

[22] A. Hodjat, I. Verbauwhede, "Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors," IEEE Trans. Comp., no. 4, pp. 366–372, 2006.

[23] S.K. Mathew, F. Sheikh, M. Kounavis, "53 Gbps native GF (24)2 composite-field AES-encrypt/decrypt accelerator for content-protection in 45 nm high-performance microprocessors," IEEE Jour. Solid-State Circuits, no. 4, pp. 767–776, 2011.

[24] J.Y. Park, O. Yi, J.S. Choi, "Methods for practical whitebox cryptography," IEEE Transaction, pp. 474–479, 2011.

[25] L. Gaspar, M. Drutarovsky, V. Fischer, N. Bochard, "Efficient AES S-boxes implementation for non-volatile FPGAS," IEEE Transaction, pp. 649–653, 2009.

[26] G.N. Selimis, A.P. Fournaris, O. Koufopavlou, "Applying low power techniques in AES MixColumn/InvMixColumn transformations," IEEE Transaction, pp. 1088–1092, 2006.

[27] S.M. Wadi, N. Zainal, "High definition image encryption algorithm based on AES modification," Springer Wireless Comm., pp. 811–829, 2014.

[28] J. Goodwin, P.R. Wilson, "Advanced encryption standard (AES) implementation with increased DPA resistance and low overhead," IEEE Transaction, pp. 3286–3289, 2008.

[29] M. J. Atallah, M. Blanton, N. Fazio, K. B. Frikken, "Dynamic and efficient key management for access hierarchies,"ACM Trans. Inf. Syst. Secur., vol. 12, no. 3, pp. 1–43, 2009.

[30] Yi Wang, A. Kumar and Y. Hay, "FPGA-based high throughput XTS-AES encryption/decryption for storage area network" National University of Singapore, Singapore, 2014.

[31] K. Rahimunnisa, P. Karthigaikumar, N.A. Christy, S.S. Kumar and J.Jayakumar, "Psp: parallel sub-pipelined architecture for high throughput AES on FPGA and ASIC," Central European Jour. of Comp. Sci., vol. 3, pp. 173-186, Dec. 2013.
[32] Q. Liu, Z. Xu and Y. Yuan. 2013, "A 66.1 Gbps single-pipeline AES on FPGA," In Proceedings of International Conference on Field Prog. Tech. (FPT), IEEE, Kyoto, pp. 378-381.
[33] V. K. Sharma, S. Kumar and K. K. Mahapatra, "Iterative and fully pipelined high throughput efficient architectures of AES in FPGA and ASIC," Jour. of Circuits, Sys., and Comp., vol. 25, pp. 1650049, May 2016.
[34] Q. Liu, Z. Xu and Y. Yuan, "High throughput and secure advanced encryption standard on field programmable gate array with fine pipelining and enhanced key expansion," IET Comp. & Digital Techq., vol. 9, pp.175-184, May 2015.
[35] Y. Wang and Y. Ha. 2016, "High throughput and resource efficient AES encryption/decryption for SANs," In Proceedings of International Symp. on Circuits and Sys., IEEE, Montreal, pp. 1166-1169.