MODIFIED ADVANCED ENCRYPTION STANDARD FOR MORE SECURE COMMUNICATION

[1]M. Bhagya Lakshmi, [2]Dr. P. Krishna Murthy

[1]M.Tech Student, [2]Associate Professor & Head,
[1, 2]Department of ECE,
[1,2] Chadalawada Ramanamma Engineering College, Tirupati, A.P. India.

Abstract: The Advanced Encryption Standard (AES) algorithm has become the default choice for various security services in copious applications. Internet of things (IoT), internetworking of smart devices, embedded with sensors, software, electronics and network connectivity that enables to communicate with each other to exchange and collect data through an uncertain wireless medium. Recently IoT devices are dominating the world by providing it's versatile functionality and real-time data communication. Apart from versatile functionality of IoT devices, they are very low battery powered, small and sophisticated, and experience lots of challenges due to unsafe communication medium. But due to recent emerge of IoT devices, the main concern are shifting to moderate security and less energy consumption rate. In existing Modification for the AES Algorithm (MAES) a new 1-dimensional Substitution Box is implemented by formulating a novel equation for constructing a square matrix in affine transformation phase of MAES where the area hardware is more. Affine transformation has scaling, translation and rotation while receiving data from satellites these operations are performed. In proposed method the mix column is replaced by random permutation. In this area is considered based on look up tales. The random permutation stage performs the XoR operation between the Linear-Feedback Shift Register (LFSR) and state matrix from shift rows. The main concern is shifting to moderate security and less area consumption. The proposed method has mainly four steps. This will improve the security level and also the area and delay will be reduced when compare to existing method.

***Index Terms* - Advanced Encryption Standard, IoT, Linear-Feedback Shift Register, MAES**

I. INTRODUCTION

Internet of Things (IoT) is the next revolution of the internet which brings profound impact on our everyday lives. IoT is the extension of the Internet to connect just about everything on the planet. This includes real and physical objects ranging from household accessories to industrial engineering. As such these “things” that are connected to the Internet will be able to take actions or make decisions based on the information they gather from the Internet with or without human interaction. In addition, they also update the Internet with real-time information with the help of various sensors. IoT works with resource-constraint components such as sensor nodes, RFID tags etc. These components have low computation capability, limited memory capacity and energy resources, and susceptibility to physical capture. Also, they communicate through the wireless communication channel which is not secured and transmit real-time information through the treacherous wireless medium.

With respect to the security aspect and implementation complexity, AES is considered as one of the strongest and efficient algorithms. Despite that like other symmetric encryption algorithms, the secret key distribution is still considered as a critical issue. Again to encrypt or decrypt a single block (128-bit) of data, an essential amount of computational processing has to be done which consumes enormous battery power. As components of IoT have resource-constraint characteristics, consuming immense power may cause expiration of such components. Analyzing related work, come to know that Substitution Layer is the most energy consuming portion of AES in the round based design. Considering energy consumption of resource-constrained components of IoT and are proposing MAES, a lightweight version of AES where reduce the computation of Substitution Box (S-Box) of AES.

The definition of the Internet of things has evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems [1]. Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", including devices and appliances (such as lighting fixtures, thermostats, home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smart phones and smart speakers. There are a number of serious concerns about dangers in the growth of IoT, especially in the areas of privacy and security, and consequently industry and governmental moves to address these concerns have begun including the development of international standards.

The applications of Advanced Encryption Standard (AES) in audio and video signals. Like the cipher text is completely different from the plaintext in AES operation, so the encrypted audio or visual signal should have the same effect. The experiments reveal the encrypted signals are so much different from the original ones that they become random noises. However, in some cases, a kind of pattern may appear within the encrypted noise in the ECB mode operation, causing a kind of sounds being heard during the play back of encrypted audio noise, or some patterns appeared amid the cipher images, due to having the same audio or video inputs which can be mostly reduced by compressing before encryption. This project presents the ways, featured in the other four modes of AES, to make the same inputs different without compressing. The high speed parallel operations for the five modes are also discussed.

II. LITERATURE SURVAY

Madakam, Somayya, R. Ramaswamy, and Siddharth Tripathi. "Internet of Things (IoT): A literature review." Journal of Computer and Communications

The Internet revolution has profoundly impacted our lives. Not only has it deeply changed the way businesses operate, but also the way lives. Today, witnessing a new technology and data-led transformation called Internet of Things (IoT) which is transforming almost every industry. It aims to unify everything in this world under one umbrella with which the things cannot just be controlled and monitored but the state of the thing could be known as well. In future Internet of Things transforms the real world objects into smart virtual objects allowing a seamless human-to machine and machine-to-machine communication. With this, present study addresses IoT concepts through methodical review of scholarly research papers, white papers and online databases. Besides this the research article focuses on definitions, chronology of IoT, pre-requisites for Internet of Things, provides an overview of IoT architectures, technologies, applications and the challenges faced in adopting it. This Thesis also revolves around the privacy and security aspect of Internet of Things which has rarely been discussed before. This Thesis helps in having a thorough understanding for beginners/researchers about the IoT.

Eisenbarth, Thomas, and Sandeep Kumar. "A survey of lightweight cryptography Implementations." IEEE Design & Test of Computers 24.6(2007).

The upcoming era of pervasive computing will be characterized by many smart devices that because of the tight cost constraints inherent in mass deployments—have very limited resources in terms of memory, computing power, and battery supply. Here, it's necessary to interpret Moore's law differently: Rather than a doubling of performance, see a halving of the price for constant computing power every 18 months. Because many foreseen applications have extremely tight cost constraints—for example, RFID in tetra packs—over time, Moore's law will increasingly enable such applications.

Beaulieu, Ray, et al. "The SIMON and SPECK lightweight block ciphers." Design Automation Conference (DAC), 52nd ACM/EDAC/IEEE. IEEE, 2015.

Cryptographic design is all about compromise. For robust security, there is a desire to use components with strong cryptographic properties, and to build in a large margin of security by stepping an algorithm many more times than may seem necessary. The competing aim efficiency—means that I want to minimize computation to the extent possible. How one balances these conflicting goals is the art of cryptography. The problem is complicated by the fact that efficiency is not a well-defined notion.

An algorithm can have efficient realizations in dedicated hardware (e.g., on an ASIC), but sacrifice performance on 8-bit microcontrollers. Or it could admit high-throughput implementations on 64-bit desktop processors, but require a large amount of code. Or it could be designed to optimize performance on a particular processor (by taking full advantage of the instruction set for that processor). Or it could be tailored for high performance on a particular FPGA (for example by basing it on LUTs of a certain size). Or it could have very high-throughput pipelined ASIC implementations, but offer no compact realization suitable for constrained devices. Whether or not an algorithm is secure may seem clearer, but there are plenty of questions here as well.

Daemen, Joan and Rijmen, Vincent. "The design of Rijndael: AES-the advanced encryption standard." , Springer Science & Business Media, 2013.

Information systems and computer networks has seen a wide spread in the last century. However, it has been realized that these systems and networks must be secured rigorously or it will not be utilized properly. This is why more than 50 countries has officially published a form of strategic document to describe their stance on cyber security issues. According to the International Telecommunication Union, cyber security includes Confidentiality, Integrity and Availability security services. In this research we shall focus on the confidentiality security service. The most commonly used mechanism to provide confidentiality is encryption.

III. EXISTING METHOD

The existing work consists of 1-dimensional Substitution Box (S-Box) which is constructed by formulating a novel equation for constructing a square matrix in affine transformation phase of MAES. In this work they have implemented both original AES and MAES algorithms to compare the work. After analyzing the result of our experiment and conclude that MAES is well efficient than milliseconds in terms of number of packet transmission and latency, respectively. In existing system they have modified the S-box in this proposed system they have modified the mix column in order to get the better area and achieve high speed. In the proposed system they have used the LFSR which generates pseudo random numbers which will improve the security level of the MAES.

A deterministic algorithm to generate a sequence of numbers with little or no discernible pattern in the numbers, except for broad statistical properties also known as PRNG, deterministic random bit generator, DRBG. The Internet of things (IoT) describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.

Careful choice must be made in selecting the mode of operation of the cipher. The simplest mode encrypts and decrypts each 128-bit block separately. In this mode, called electronic code book (ECB), blocks that are identical will be encrypted identically; this is entirely insecure. It makes some of the plaintext structure visible in the ciphertext. Selecting other modes, such as using a sequential counter over the block prior to encryption (i.e., CTR mode) and removing it after decryption avoids this problem. Another mode, Cipher Block Chaining (CBC) is one of the most commonly used modes of AES due to its use in TLS. CBC uses a random initialization vector (IV) to ensure that distinct ciphertexts are produced even when the same plaintext is encoded multiple times. The IV can be transmitted in the clear without jeopardizing security.

IV. Advanced Encryption Standard

The Advanced Encryption Standard (AES), a symmetric key block which is published by the National Institute of Standards and Technology (NIST) in December 2001. It is a non-Feistel block cipher that encrypts and decrypts a fixed data block of 128-bits.

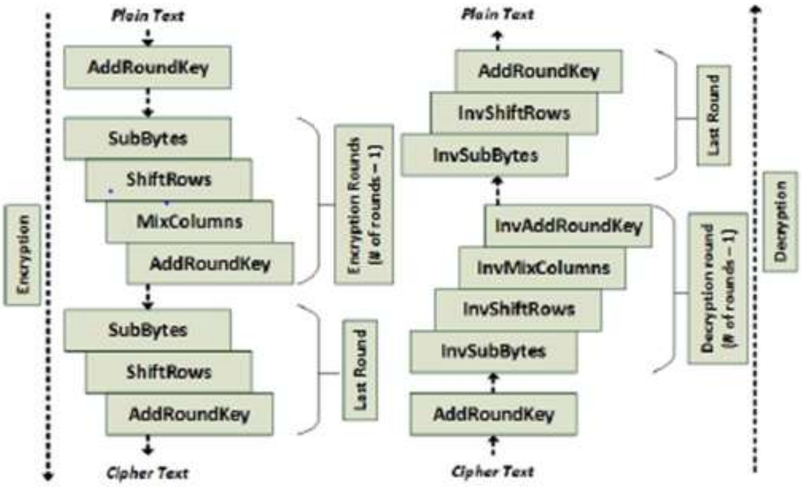

Figure 1: General Design of AES Encryption and Decryption

There are three different key lengths. The encryption/decryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.AES performs several rounds where each round is made of several stages. A data block is transformed from one stage to another. Before and after each stage, the data block is referred to as a state. Each round, except the last, performs four transformations which are invertible. The last round implements the rest three transformations except the Mix Columns stage. Figure 1 shows the AES cipher structure.

Modified Advanced Encryption Standard:

According to previous research observation, found that S-Box and Mix Columns are the most energy consuming stages in encryption and decryption process. Analyzed the S-Box generation process of the Rijndael AES. The 16x16 2-dimensional lookup table is formed through the multiplicative inverse phase and affine transformation phase in the original AES. Proposing a new 1-dimensional lookup table as S-Box. It also follows the same generation process as the original one. However, substitution of one complete byte requires two times substitution from the SBox. First four bits of the state byte is replaced first then the remaining four bits are substituted from the S-Box.

Rijndael S-Box Generation Method: The Rijndael S-Box is a square matrix which is used in the Rijndael cipher. The S-Box serves as a lookup table. It is generated by determining the multiplicative inverse for a given number in GF(28) and then transforming the multiplicative inverse using affine transformation.

1) Multiplicative Inverse Phase: In multiplicative inverse phase, the input byte is inversed by substituting value from multiplicative inverse table.
2) Affine Transformation: Selection of the irreducible polynomial and the designated byte are the two most important factors of affine transformation phase. In Rijndael AES,x8 + x4 + x3 + x + 1 is used as the irreducible polynomial and as the constant column matrix 0x63 specially designated byte is chosen. Basically, the affine transformation consists of two operations. Firstly, 8x8 square matrix's multiplication and secondly, 8x1 constant column matrix addition. The 8x8 square matrix is constructed using the following

$$d_i = b_i\_b(i+4)\%8\_b(i+5)\%8\_b(i+6)\%8\_b(i+7)\%8\_C_i \qquad (1)$$

where

bi =ith bit of multiplicative inverse of input byte

C_i = ith bit of a specially designated byte

Figure 2 illustrates the generation process of Substitution Box (S-Box) of the original AES.

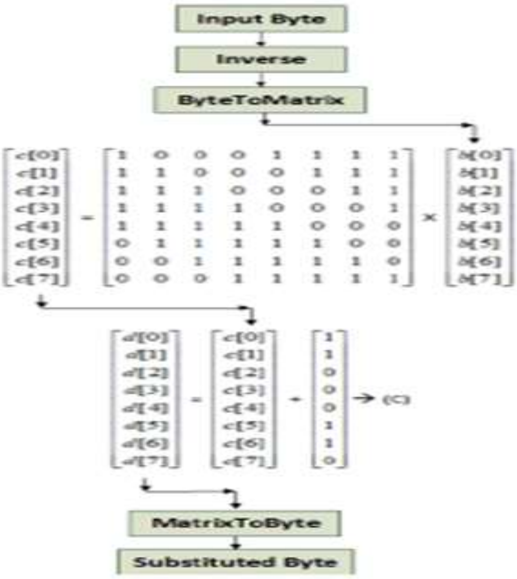

Figure 2: Original S-Box generation process

Modified AES S-Box Generation

Our modified AES S-Box generation process follows the construction procedure of the original AES. The whole process differs only in the selection of the irreducible polynomial and specially designated byte.

Multiplicative Inverse Table: In the Rijndael AES, all the arithmetic operations are performed over the Galois Field. In our work, the Galois Field is considered. The number of irreducible polynomials of degree 4 over GF are x4 + x + 1, x4 + x3 + x2 + x + 1 and x4 + x3 + 1.

Different S-Boxes and inverse S-Boxes for different values of the constant value C is given below from figure 9 to 13:

Table 1: Case-1: When C = 0x03

Case 1: When C = 0x03

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3	4	F	B	2	1	7	0	C	D	5	9	6	E	A	8

Table 2: Case-2: When C = 0x08

Case 2: When C = 0x08

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
8	F	4	0	9	A	C	B	7	6	E	2	D	5	1	3

The fixed point refers to the generation of the output value same as the input value.

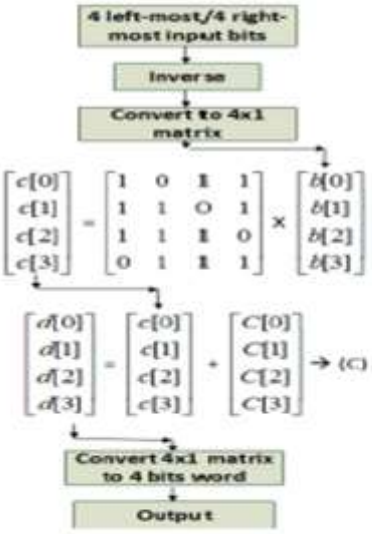
4 left-most/4 right-most input bits
Inverse
Convert to 4x1 matrix
→ (C)
Convert 4x1 matrix to 4 bits word
Output

Figure 3: Proposed MAES S-Box generation process

All the generated values of the multiplicative inverse table and substitution box depend on the selection of irreducible polynomial. For our experiment purpose, choose x4+x+1 as our irreducible polynomial and can select any of the irreducible polynomials which are mentioned above. Following the Extended Euclidean Algorithm, 1-dimensional multiplicative inverse table is formed. Figure 3 shows the generation process of proposed MAES.

V. Proposed Method

Modifying the AES algorithm has been done several times before, each researcher limits his concerns to one characteristic to improve. The main characteristics that the researchers concentrate on are the speed of the AES. In existing method they have modified the s-box for the better performance but the area and delay are complex. our proposed design will improve the performance in terms of area and delay.

Increasing the speed of the AES algorithm, while keeping the security level high is a vital for a lot of applications that require high security level with limited resources. The AES algorithm explained in the previous method suffers from consumption of unnecessary time to achieve the necessary complexity needed to meet the security level. A new Modification for the AES

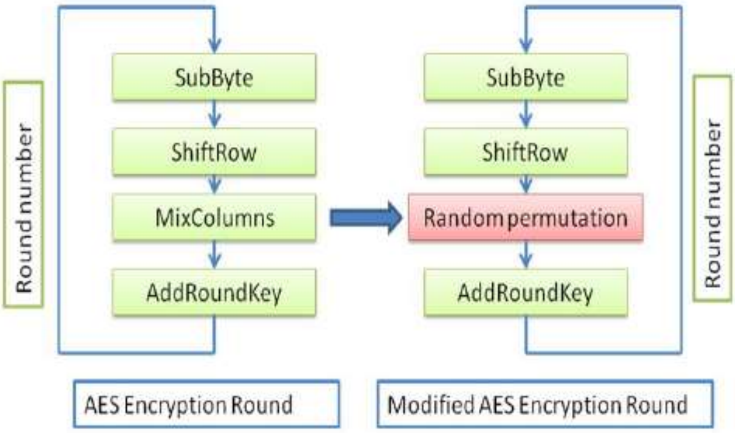

Figure 4: The proposed MAES Algorithm compared with AES Algorithm Design

Algorithm (MAES) is done changing the s-box as well as by replacing the Mix Columns stage with random number generator. This will increase the speed of the algorithm without a decrease in the security of the AES algorithm. In addition, the security of the MAES algorithm can be enhanced using the permutation stage which uses random number generator.

The design of the MAES algorithm will ensure the following:

1. Speed up the AES algorithm by replace Mix Columns stage with simple xor operations.
2. To the xor operation the first input is state matrix coming from shift rows.
3. The second input for the Xor operation is random number generator like linear feedback shift register.

In the above figure 4 mix column is replaced by the random permutation. The random permutation consists of xor operation between the state matrix and the random number generator. LFSR is used as a random number generator.

Random Number Generator:

Linear-Feedback Shift Register (LFSR) is a shift register whose input bit is a linear function of its previous state. The most commonly used linear function of single bits is exclusive-or (XOR). Thus, an LFSR is most often a shift register whose input bit is driven by the XOR of some bits of the overall shift register value. An LFSR is a class of devices known as state machine. It is a shift register whose input bit is a linear function of its previous state. The only linear functions of single bits are XOR and XNOR. Thus it is a shift register whose input bit is driven by XOR or XNOR of some bits of overall shift register value. LFSR used in this work is 128-bit with maximum length feedback polynomial$x^{128} + x^{127} + x^{126} + x^{121} + 1$ for which2^{128}-1 = 429, 49, 67,295 random outputs.

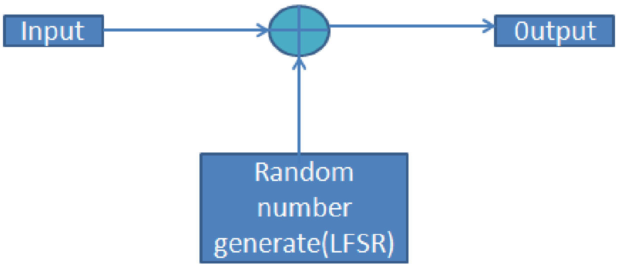

Figure 5: Random Permutation Stage

The above figure 4.2 shows the random permutation stage which consists of one input from the shift rows and another input from the 128 bit LFSR .The xor operation is performed from this two inputs and generate the random output which will act as input to the add round stage.

It works mainly based on 4 steps

1. Substitute Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key

Modified Subbytes Transformation:

AES Sub Bytes transformation was modified to make it round key dependent; this is to ensure that a change in the key is easily discovered in the cipher text. To achieve that, the 16 bytes round key was used to obtain four eight-bit keys XORkey0, XORkey1, XORkey2, XORkey3 by XORing all the bytes of the corresponding row (Row i) in the round key matrix, as shown in Equation (2). After obtaining the XOR keys, each XOR key i as shown in Equations (3)–(6) was then added to all of the bytes in the corresponding row (Row i) of the state matrix before substituting the values in the S-Box. Mathematically, given the state S and a round key K, represented as a 4 × 4 matrices:

$$S = \begin{array}{|c|c|c|c|}\hline S\ 0,0 & S\ 0,1 & S\ 0,2 & S\ 0,3 \\ \hline S\ 1,0 & S\ 1,1 & S\ 1,2 & S\ 1,3 \\ \hline S\ 2,0 & S\ 2,1 & S\ 2,2 & S\ 2,3 \\ \hline S\ 3,0 & S\ 3,1 & S\ 3,2 & S\ 3,3 \\ \hline \end{array} \quad \text{and } K = \begin{array}{|c|c|c|c|}\hline K0,0 & K0,1 & K0,2 & K0,3 \\ \hline K1,0 & K1,1 & K1,2 & K1,3 \\ \hline K2,0 & K2,1 & K2,2 & K2,3 \\ \hline K3,0 & K3,1 & K3,2 & K3,3 \\ \hline \end{array}$$

The operation can be seen clearly from the matrix below:

$$S' = \begin{array}{|c|c|c|c|}\hline S_{0,0} \oplus Key_0 & S_{0,1} \oplus Key_0 & S_{0,2} \oplus Key_0 & S_{0,3} \oplus Key_0 \\ \hline S_{1,0} \oplus Key_1 & S_{1,1} \oplus Key_1 & S_{1,2} \oplus Key_1 & S_{1,3} \oplus Key_1 \\ \hline S_{2,0} \oplus Key_2 & S_{2,1} \oplus Key_2 & S_{2,2} \oplus Key_2 & S_{2,3} \oplus Key_2 \\ \hline S_{3,0} \oplus Key_3 & S_{3,1} \oplus Key_3 & S_{3,2} \oplus Key_3 & S_{3,3} \oplus Key_3 \\ \hline \end{array}$$

The resultant state matrix *S′* is given as follows:

$$S' = \begin{array}{|c|c|c|c|}\hline S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ \hline S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ \hline S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ \hline S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \\ \hline \end{array}$$

After obtaining the new state matrix *S′*, the bytes are then substituted in the substitution table (S-Box) using normal Sub Bytes operation, as shown in Equation (8): S'i,j=SubstitutionBox[S'i,j], where j = 0 to 3 for every i = 0 to 3. The strength of a cryptographic algorithm can be determined by measuring its diffusion and confusion property while using the avalanche effect. The term avalanche effect was first used by Horst Feistel in his article titled “Cryptography and Computer Privacy” published in 1973. Later, the concept was identified as Shannon’s property of confusion. The avalanche effect is used to measure the amount of randomness (non-linearity) of hash functions and cryptographic algorithm, especially block ciphers, such as Data Encryption Standard (DES) and Advance Encryption Standard (AES).

Modification to the Shift Rows operation was achieved by randomizing the entire operation. In the conventional AES algorithm, the Shift Rows operation depends on a fixed number, called the offset, which determines the number of byte position(s) each row of the state will be shifted. With this modification, the operation does not have to depend on the fixed offset, it now depends on a number, called the Rank Number (*RNo*), which is obtained by manipulating each row of the state matrix with the corresponding row of the round key matrix. The rows of the state are shifted based on the rank number obtained. To obtain the rank number using a state matrix *S* and a round key matrix *K*, the following steps were adopted:

$$S= \begin{array}{|c|c|c|c|}\hline S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ \hline S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ \hline S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ \hline S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \\ \hline \end{array} \quad \text{and } K = \begin{array}{|c|c|c|c|}\hline K_{0,0} & K_{0,1} & K_{0,2} & K_{0,3} \\ \hline K_{1,0} & K_{1,1} & K_{1,2} & K_{1,3} \\ \hline K_{2,0} & K_{2,1} & K_{2,2} & K_{2,3} \\ \hline K_{3,0} & K_{3,1} & K_{3,2} & K_{3,3} \\ \hline \end{array}$$

Step 1: Each row (Rowi) of the state matrix was added to the corresponding row in the round key matrix using XOR to obtain a 4-byte vector called State-Key (SKey) vector.
Step 2: The four-byte of the State-Key vector are then XORed together to obtain an 8-bit value called the Rank Value (RVal).
Step 3: The eight-bit Rank Value (RVali) is then stored in corresponding Rowi of the state matrix.
Step 4: Steps 1–3 will be repeated for the remaining rows Row1 to Row3
Step 5: Attach Rank Number (RNo) to the Rank Values obtained in Step 3 above for each of the rows of the state (Row0 to Row3) in ascending order with the minimum rank value having 1 as the rank number while the maximum rank value has 4 as the Rank Number.

If a cryptographic algorithm does not exhibit a significant degree of avalanche effect (at least 50%), then that algorithm has poor randomization. Thus, cryptanalysts can make predictions about the input, only being given the output. This may be enough to partially or worst, completely break the algorithm. In addition to the avalanche effect, the time taken for encryption and decryption were also measured.

VI. Results

Proposed MAES:

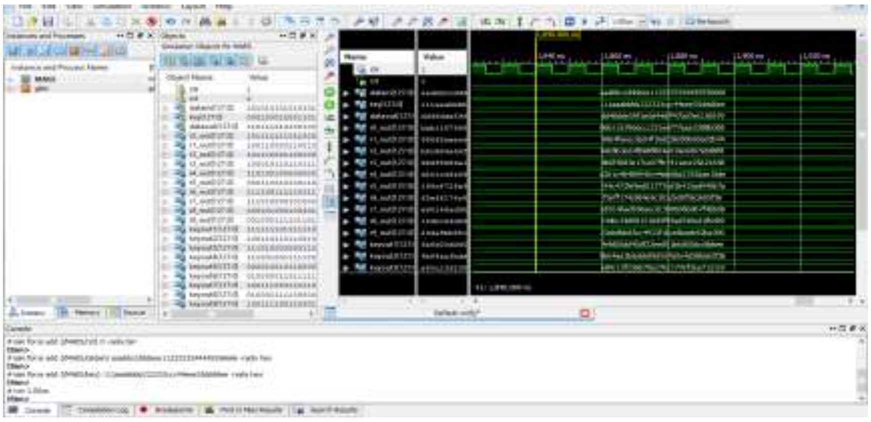

Figure 6: Results of Proposed MAES

Table 3: Comparison of Existing and Proposed Method

	Area(LUT)	Delay(in ns)
Existing Method	4281	30.263
Proposed Method	2626	18.436

In the figure 6 it was shown that for 128 bits inputs is given and 128 bits random key is given as another input and the outputs as key outs from 1 to 9 was observed. In the we observed that delay was removed because in final stage one step is reduced and area is reduced. Here we observed that area reduction in the form of number of LUT's. The comparisons are shown in the table 3.based on those improved results we have more advantages.

Conclusion

One of the widely used algorithms is advance encryption standard (AES), this algorithm suffer from consuming unnecessary time to achieve the complexity requirements needed for the encryption process specially for the real time application. Several modifications have been done on the algorithm to reduce the consuming time or to increase the complexity of the algorithm, but all the modification concentrate on one purpose which is decrease the consumption time or increase the complexity of the algorithm. In existing system a new s-box is proposed. In this proposed work, a new modification is applied on the AES algorithm by replacing the mix column with random permutation. The new algorithm which is called MAES can increase the speed of the algorithm processes and decreasing the area , while maintaining the complexity of the encryption as high as possible when compare to existing method.

References

[1] Madakam, Somayya, R. Ramaswamy, and SiddharthTripathi. "Internetof Things (IoT): A literature review." Journal of Computer and Communications 3, no. 05 (2015): p.164.

[2] Wang, Yong, GarhanAttebury, andByrav Ramamurthy. "A survey of security issues in wireless sensor networks." IEEE Communications Surveys Tutorial (2006).

[3] Veeramallu, B., S. Sahitya, and ChLavanyaSusanna. Veeramallu, B., S. Sahitya, and ChLavanyaSusanna. "Confidentiality in Wireless sensor Networks." International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.

[4] Eisenbarth, Thomas, and Sandeep Kumar. "A survey of lightweightcryptographyimplementations." IEEE Design & Test of Computers 24.6 (2007).

[5] Banik, Subhadeep, AndreyBogdanov, and Francesco Regazzoni. "Exploring energy efficiency of lightweight block ciphers." International Conference on Selected Areas in Cryptography. Springer, Cham, 2015.

[6] Bogdanov, Andrey, et al. "PRESENT: An ultra-lightweight block cipher." CHES. Vol. 4727. 2007.

[7] Borghoff, Julia, et al. "PRINCEa low-latency block cipher for pervasive computing applications." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2012.

[8] Beaulieu, Ray, et al. "The SIMON and SPECK lightweight block ciphers." Design Automation Conference (DAC), 52nd ACM/EDAC/IEEE. IEEE, 2015.

[9] Suzaki, Tomoyasu, et al. "TWINE: A Lightweight Block Cipher for Multiple Platforms." Selected Areas in Cryptography. Vol. 7707. 2012.

[10] Li, Wei, et al. "Security analysis of the LED lightweight cipher in the internet of things." JisuanjiXuebao(Chinese Journal of Computers) 35.3 (2012): p.434-445.

[11] Shibutani, Kyoji, TakanoriIsobe, HarunagaHiwatari, Atsushi Mitsuda, Toru Akishita, and TaizoShirai. "Piccolo: An ultra-lightweight blockcipher." In CHES, vol. 6917, pp. 342-357. 2011.

[12] Wu, Wenling, and Lei Zhang. "LBlock: a lightweight block cipher." In Applied Cryptography and Network Security, pp. 327-344. Springer Berlin/Heidelberg, 2011.

[13] Daemen, Joan and Rijmen, Vincent. "The design of Rijndael: AES-theadvanced encryption standard.", Springer Science & Business Media, 2013.

[14] Al Hasib, Abdullah, and Abul Ahsan MdMahmudulHaque. "A comparative study of the performance and security issues of AES and RSA cryptography." Third International Conference on Convergence and Hybrid Information Technology, 2008. Vol.2.

[15] Feldhofer, Martin, Johannes Wolkerstorfer, and Vincent Rijmen. "AES implementation on a grain of sand." IEE Proceedings-Information Security 152, no. 1 (2005): p.13-20.

[16] Moradi, Amir, Axel Poschmann, San Ling, ChristofPaar, and HuaxiongWang. "Pushing the limits: a very compact and a threshold implementation of AES." In Eurocrypt, vol. 6632, pp. 69-88. 2011.

[17] Hocquet, Cdric, Dina Kamel, Francesco Regazzoni, Jean-Didier Legat, Denis Flandre, David Bol, and Franois-Xavier Standaert. "Harvesting the potential of nano-CMOS for lightweight cryptography: an ultra-lowvoltage65 nm AES coprocessor for passive RFID tags." Journal of Cryptographic Engineering 1, no. 1 (2011): p.79-86.

[18] Kerckhof, Stphanie, FranoisDurvaux, CdricHocquet, David Bol, and Franois-Xavier Standaert. "Towards green cryptography: a comparison of lightweight ciphers from the energy viewpoint." Cryptographic Hardware and Embedded SystemsCHES 2012 (2012): p.390-407.

[19] Batina, Lejla, et al. "Dietary recommendations for lightweight block ciphers: power, energy and area analysis of recently developed architectures." International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer, Berlin, Heidelberg, 2013.