A Verilog Implementation of MAES Using Xilinx Software for Resource Constraint Environments

[1]Akash Kumar, [2]Dr. Bharti Chourasia
[1]M.Tech Scholar, [2]Professor & HOD
[1]Department of Electronics & Communication,
[1]RKDF Institute of Science & Technology Bhopal, India.

Abstract : Advance Encryption Standard (AES) is considered as one of the secure 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 more power. Internet of things (IoT) is the extension of the Internet to connect just about everything on the planet. This paper presents verilog Implementation of Modified Advanced Encryption Standard Algorithm using Xilinx Software. MAES is a lightweight version of AES which meets the demand. A new one-dimensional substitution Box (S-box) is proposed instead of conventional 2-D S-box and previous 1-D S-box. Simulated result shows that proposed MAES gives better performance than previous MAES in term of delay, throughput, transmission time, efficiency rate.

IndexTerms **–**IOT, Wireless, Security, Cryptography, Encryption, Decryption, Block Cipher, Simulation, Synthesis, Xilinx.

I. INTRODUCTION

5G is the fifth era of cell portable interchanges. It succeeds the 4G (LTE/WiMax), 3G (UMTS) and 2G(GSM) frameworks. Internet of Things security is the area worried about ensuring interconnected gadgets and systems in the biological community. In an IoT biological system registering gadgets and installed frameworks, likewise called things can impart information over system as they are furnished with special identifiers and capacity to gather, send and get information. IoT applications can be found in all divisions extending from home apparatuses to mechanical machine-to-machine (M2M) to shrewd vitality matrices. The individual data gathered and put away with these gadgets —, for example, your name, age, wellbeing information, area and that's just the beginning — can help crooks in taking your personality. In the meantime, the internet of Things is a developing pattern, with a surge of new items hitting the market. Be that as it may, here's the issue: When you're associated with everything, there are more approaches to get to your data. That can make you an alluring focus for individuals who need to make a benefit off of your own data. Every associated gadget you possess can include another protection concern, particularly since the vast majority of them interface with your cell phone. Here's the manner by which it works. Regardless of whether you have to check the cameras in your home, bolt or open an entryway, modify temperature or lighting, pre-warm the broiler, or kill a television, you can do everything remotely with only a couple of taps on your cell phone. Be that as it may, the more functionality you add to your cell phone, the more data you store in the gadget. This could make cell phones and anything associated with them helpless against a huge number of various kinds of assaults. The exchange of digital data over a network has exposed the multimedia data to various kinds of abuse such as Brute-Force attacks, unauthorized access, and network hacking. Therefore, the system must be safeguarded with an efficient media-aware security framework such as encryption methods that make use of standard symmetric encryption algorithms, which will be responsible for ensuring the security of the multimedia data. For the encryption of electronic data, one of the most prominent cryptographic algorithms is the Advanced Encryption Standard algorithm.

The Advanced Encryption Standard (AES) has been lately accepted as the symmetric cryptography standard for confidential data transmission. However, the natural and malicious injected faults reduce its reliability and may cause confidential information leakage. In this paper, we study concurrent fault detection schemes for reaching a reliable AES architecture. Cryptography is the science of secret codes, enabling the confidentiality of communication through an insecure channel. It protects against unauthorized parties by preventing unauthorized alteration of use. Generally speaking, it uses a cryptographic system to transform a plaintext into a cipher text, using most of the time a key. As networking technology advances, the gap between network bandwidth and network processing power widens. Information security issues add to the need for developing high-performance network processing hardware, particularly that for real-time processing of cryptographic algorithms.

AES is basically a security algorithm is used for encryption and decryption of data. Encryption is the process in which we perform a fixed set of operation on the data to randomize the data and transform it into some meaningless form so that even if any unauthorized agents gets an access of the data, will not be able to obtain the useful information present in the data. Such data which is apparently meaningless is transmitted. Such data can be converted back to its useful form, that is, the actual data only with the key of the key at the receiving end. Keys are basically a secret binary data of above said fixed length which are used to encrypt (cipher) the original data at the transmitting end to obtain the encrypted data and decrypt (de-cipher) the encrypted data to get back the original data at the receiving end. Its obvious that the key with the help of which the data will be retrieved at the receiving end will be known at the receiving end prior to the establishment of the communication. This process of retrieving the original data is called decryption. The branch of science which deals with encryption and decryption of data is known as Cryptography. The algorithms with the help of which we implement encryption or decryption of data are called Cryptographic algorithms.

II. PROPOSED APPROACH

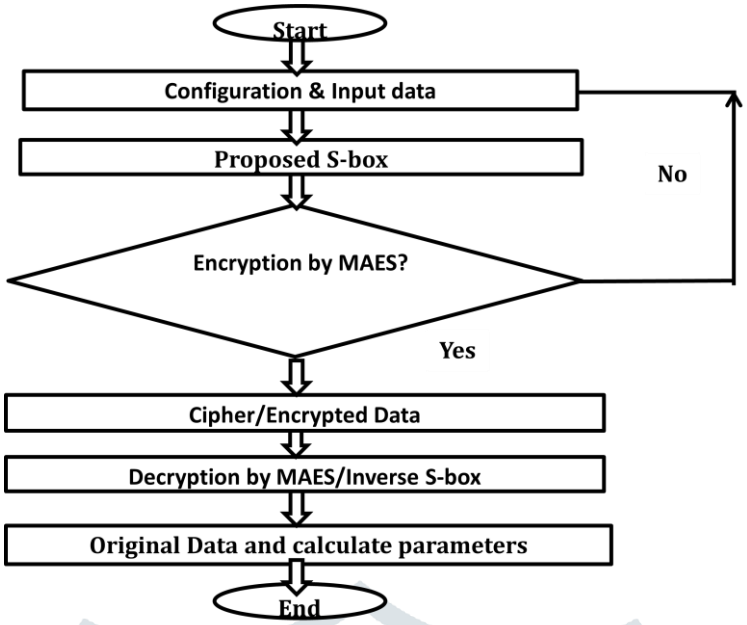

Figure 1: Flow Chart

Cryptographic algorithms can be either symmetric or non-symmetric. Symmetric Cryptographic algorithms are those in which we use the same set of keys both at the transmitting end as well as the receiving end. AES is a symmetric block cipher. AES Algorithm may be used with the three different key lengths of 128,192 and 256. AES is referred to as "AES-128", "AES-192", and "AES-256" accordingly. In the proposed work we have used AES-128. Thus, symmetric cipher requires a single key for both encryption and decryption, which is independent of the plaintext and the cipher itself. Hence, it would be impractical to retrieve the plaintext solely based on the cipher text and the decryption algorithm, without knowing the encryption key. Thus, the secrecy of the encryption key is of high importance in symmetric ciphers such as AES.

AES can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, or 256 bits. In the proposed work, the key length is 128 bits. Rijndael was designed to handle additional block sizes and key lengths, and however they are not adopted in this standard. The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The 128 bit data block is divided into 16 bytes. These bytes are mapped to a 4×4 array called the state and all the internal operation can be performed on state. Internally, the AES algorithm's operations are performed on a two-dimensional array of bytes called the State. The encryption process includes the following transformations of states: SubBytes(), ShiftRows(), MixColumns(), and AddRoundKey(). The encryption process also includes a key schedule. The AES algorithm takes the Cipher Key, K, and performs a Key Expansion routine to generate a key schedule. In the decryption process, the Cipher transformations are inverted and then implemented in reverse order to produce a straightforward Inverse Cipher for the AES algorithm. The individual transformations used in the Inverse Cipher are InvShiftRows(), InvSubBytes(), InvMixColumns(), and AddRoundKey() . The decryption process also includes a key schedule similar to Encryption process.

In this paper, we have implemented WiMax/IOT Security using Modified Advanced Encryption Standard Cryptographic Algorithm. It is designed WiMax MAES Security Algorithm sub-module , both at the Encryption and Decryption end, based on the internal operations of the algorithm, as mentioned above. Each sub-module is designed, simulate and synthesized step by step as per algorithm. The results of simulation and synthesis are presented separately.

III. SIMULATION RESULT

The designed WiMax/IOT MAES Security Algorithm implementation has multiple sub-modules inside it both at the Encryption and Decryption end, based on the internal operations of the algorithm. Top module is designed, simulated and synthesized as per proposed algorithm. First we are presenting the results of simulation.

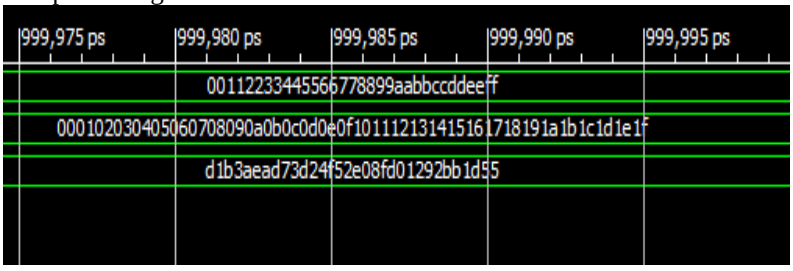

Figure 2: Encryption process

In figure 2, firstly take 128 bit in input, in hexa form it is 00112233-445566778899aabbccddeeff. Then encrypted with secure key and generate cipher form of data.

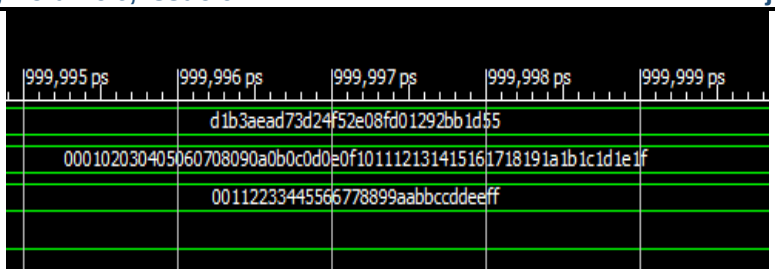

Figure 3: Decryption Process

In figure 3, take 128 bit in input, in hexa form it is d1b3aead73d24f524f2e08fd1292bb1d55. Then decrypted with inverse secure key and generate plain input i.e. 00112233-445566778899aabbccddeeff.

IV. SYNTHESIS RESULTS

RTL Schematic is the output of synthesis tool corresponding to the code that is being synthesized. It is pictorial representation of the synthesized circuit. RTL View generated initially can be used to obtain further inner level view. This is obtained by clicking on each of the representations obtained. We have obtained five RTL views from outer to inner views. As discussed earlier, the designed WiMax AES Security Algorithm implementation has multiple sub-modules inside it both at the Encryption and Decryption end, based on the internal operations of the algorithm. Each sub-module is designed, simulated and synthesized step by step as per algorithm. The simulation results is presented in the earlier part, now here, we present the results of synthesis. Please note that RTL view is Technology specific and hence little understandable from preliminary research and utility purpose.

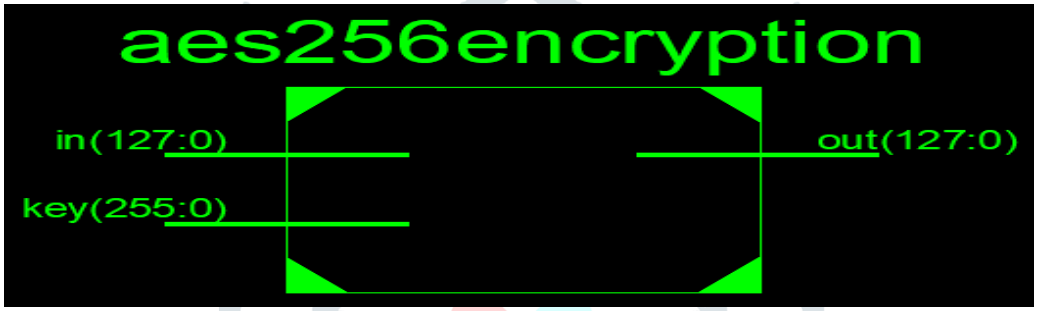

Figure 3: RTL Schematics of WiMax/IOT MAES

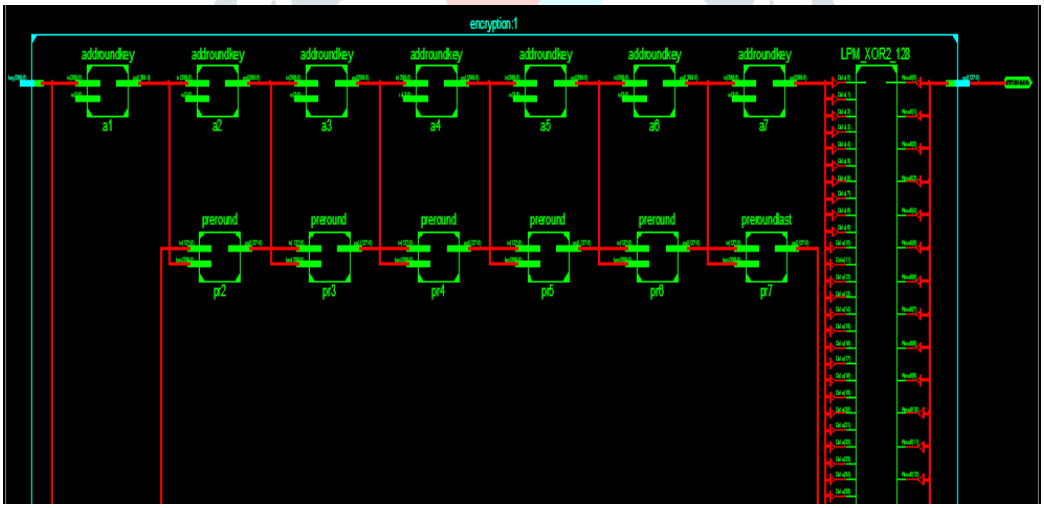

Figure 4: RTL view of proposed MAES algorithm

It is designed WiMax/IOT Security using Advanced Encryption Standard Cryptographic Algorithm. We have used Verilog for this purpose. We have used Xilinx ISE which have given synthesis results, as summarized in Table 1. Below. Also, we have depicted the pictorial representation of the results, which is the screenshot of tool generated Design Summary of individual sub-modules both at the WiMax data Encryption end and WiMax data Decryption end.

Table 1: Result Comparison of Proposed work with Previous work

Sr No.	Parameters	Previous Result	Proposed Result
1	Software	nesC	Xilinx 14.7
2	Language	Structured programming	Verilog
3	Transmission time	4969.896 milli sec	2903.02 milli sec
4	Latency	29.983 milli sec	20.380 milli sec
5	Packet	1000	1000
6	Efficiency rate	18.35%	23.7%

7	Delay	29.983 milli sec	20.380milli sec
8	Voltage	1.5 V	1.2V

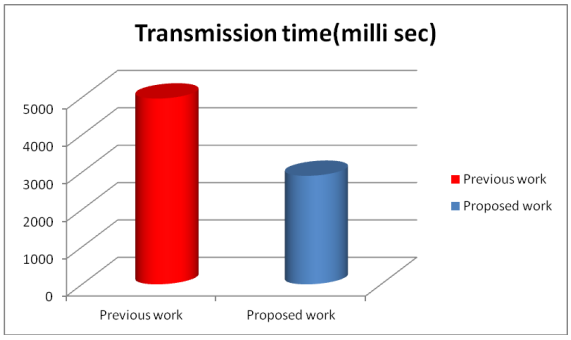

Figure 5: Transmission time comparison

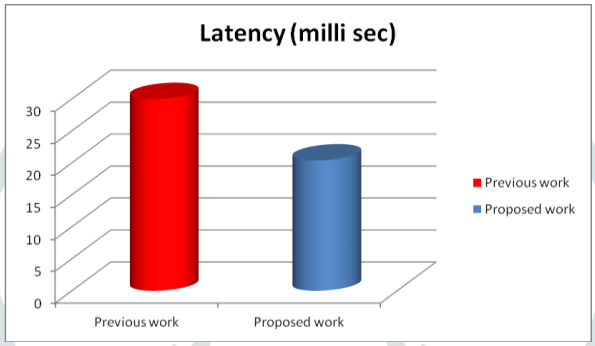

Figure 6: Delay comparison

Figure 5 and 6 showing graphical representation of transmission time and delay comparison. Therefore it is clear that proposed MAES gives better performance than previous MAES.

In this work, we have developed different modules involved in the WiMax AES encryption and Decryption for WiMax data. Mixed type of modeling is used for this purpose. The code has been optimized so that it generates lesser hardware as is evident from the Design Summary and Synthesis Report.

V. CONCLUSION

This paper proposed Modified advance encryption standard. It is optimized and Synthesizable using verilog code in Xilinx software. It is developed for the implementation of both encryption and decryption process. Each program is tested with some of the random values and output results are perfect with minimal delay. Therefore, MAES can indeed be implemented with reasonable efficiency on an FPGA, with the encryption and decryption taking an average of 32 and 34 ns respectively (for every 128 bits). MAES, a lightweight version of Advanced Encryption Standard (AES) which meets the demand. A new one-dimensional Substitution Box is proposed by formulating a novel equation for constructing a square matrix in affine transformation phase of MAES. Efficiency rate of MAES is around 23.7% in terms of packet transmission which indicates MAES consumes less energy than AES, 38.117ns latency achieved and it can be applicable for Internet of Things application.

REFERENCES

1. A. R. Chowdhury, J. Mahmud, A. R. M. Kamal and M. A. Hamid, "MAES: Modified advanced encryption standard for resource constraint environments," *2018 IEEE Sensors Applications Symposium (SAS)*, Seoul, 2018, pp. 1-6.
2. N. Gaur, A. Mehra and P. Kumar, "Enhanced AES Architecture using Extended Set ALU at 28nm FPGA," *2018 5th International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, 2018, pp. 437-440.
3. R. Paul and S. Shukla, "Partitioned security processor architecture on FPGA platform," in *IET Computers & Digital Techniques*, vol. 12, no. 5, pp. 216-226, 9 2018.
4. R. Lumbiarres-López, M. López-García and E. Cantó-Navarro, "Hardware Architecture Implemented on FPGA for Protecting Cryptographic Keys against Side-Channel Attacks," in *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 898-905, 1 Sept.-Oct. 2018.
5. T. Phan, V. Hoang and V. Dao, "An efficient FPGA implementation of AES-CCM authenticated encryption IP core," *2016 3rd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS)*, Danang, 2016, pp. 202-205.
6. P. N. Khose and V. G. Raut, "Implementation of AES algorithm on FPGA for low area consumption," *2015 International Conference on Pervasive Computing (ICPC)*, Pune, 2015, pp. 1-4.
7. S. S. H. Shah and G. Raja, "FPGA implementation of chaotic based AES image encryption algorithm," *2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA)*, Kuala Lumpur, 2015, pp. 574-577.
8. Abhiram L S, Sriroop B K, Gowrav L, Punith.Kumar H L and M. C. Lakkannavar, "FPGA implementation of dual key based AES encryption with key Based S-Box generation," *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2015, pp. 577-581.

9. S. S. S. Priya, P. Karthigai Kumar, N. M. SivaMangai and V. Rejula, "FPGA implementation of efficient AES encryption," *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, 2015, pp. 1-4.
10. 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," in *IET Computers & Digital Techniques*, vol. 9, no. 3, pp. 175-184, 5 2015.
11. Bilgin, B. Gierlichs, S. Nikova, V. Nikov and V. Rijmen, "Trade-Offs for Threshold Implementations Illustrated on AES," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 7, pp. 1188-1200, July 2015.
12. J. Senthil Kumar and C. Mahalakshmi, "Implementation of pipelined hardware architecture for AES algorithm using FPGA," *2014 International Conference on Communication and Network Technologies*, Sivakasi, 2014, pp. 260-264.
13. M. S. Kumar and S. Rajalakshmi, "Notice of Violation of IEEE Publication Principles
High efficient modified mixcolumns advanced encryption standard using Vedic multiplier," *Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014*, Coimbatore, 2014, pp. 462-466.
14. M. Atteya and A. H. Madian, "A hybrid Chaos-AES encryption algorithm and its impelmention based on FPGA," *2014 IEEE 12th International New Circuits and Systems Conference (NEWCAS)*, Trois-Rivieres, QC, 2014, pp. 217-220.
15. A. Abed and A. A. Jawad, "FPGA implementation of a modified advanced encryption standard algorithm," *2013 International Conference on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE)*, Mosul, 2013, pp. 46-51.