Design of High Speed Advanced Encryption Standard using PPA and PPM

Gajula Lakshminarayana, Anupama A. Deshpande, Moparthy Gurunadha Babu

Abstract— ***Basically, internet security plays crucial role in past three decades. So in worldwide Advanced Encryption Standard (AES) algorithm is used. AES consists of symmetric block cipher blocks. In this paper we proposed the simplified AES algorithm (S-DES) using parallel prefix adder (PPA) and parallel prefix multiplier (PPM). This parallel prefix adder and parallel prefix multiplier will generate a product formed by multiplying the multiplicand. This algorithm possess specific structure to encrypt and decrypt delicate information and is connected in equipment and programming everywhere throughout the world. It is amazingly hard to programmers to get the genuine information while encoding the AES calculation. The fundamental goal of this algorithm is to build up a model that is executed for correspondence reason, and to test the created model regarding precision reason. The encryption procedure comprises the mix of different traditional methods, for example, substitution, improvement and change encoding strategies. At last the key extension module will comprise the quantity of iterative preparing rounds so as to expand its resistance against unapproved assaults.***

Index Terms— ***Cryptography, S-AES (simplified Advanced Encryption Standard), Encryption.***

I. INTRODUCTION

Web communication is expecting the basic employment to trade extensive proportion of data in various fields. Some of data might be transmitted through channel from sender to receiver. Cryptography is the examination of data and correspondence security. Cryptography is the examination of mystery codes, empowering the Assurance of correspondence through a faulty channel. It ensures against unapproved parties by Keeping up a vital separation from unapproved change of utilization. Basically in advanced encryption standard four transformations are used. They are added round key, sub bytes, shift row and mix columns. All these four transformations depend upon the variants and length of iterations key. Each transformation can performs its operation only once except in last round. AES is a cryptographic structure which changes a plaintext into cipher content [1].

Compared to other systems, this system checks the information from assailants by utilizing two fundamental strategies that are Encryption and Decryption. Encryption is nothing but encoding the information or message. In this stage we change the information of Plain text into cipher strategy known as Cipher content. Decryption is reverse of encryption.

The system will change the content of Plain substance without missing any words in the essential substance. To play out this strategy cryptography depends upon intelligent security key near to several substitutions and changes with or without a key.

Basically, Side Channel Attacks are a kind of crypt analysis that does not concentrate on breaking the related cipher obviously but rather on discovering vulnerabilities found in certain execution of a cipher. AES in addition utilizes very surprising look up tables to create its execution. From execution we can observe that the table takes more time. So to issue encoding times it should adjust the information content and hence the key utilized for encoding. Each encoding and interpreting strategy has 2 points of view.

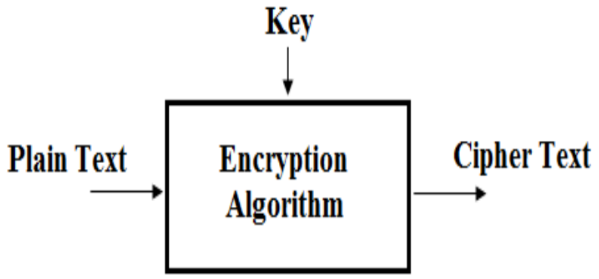


Fig.1: AES input/output parameters

The above figure (1) demonstrates the block diagram of AES information and output parameters. In this plain substance, plain text and keys are used. Present day cryptography gives the grouping, no renunciation and affirmation. Nowadays, the calculations are encoded and translated by using three sorts. Beginning one is normal cryptography that is a practically identical key's utilized for mystery composing and unscrambling data. Other is uneven crypto logical. These sorts of cryptography depend upon 2 particular keys mystery composing and unscrambling. These keys will improve the security levels of data. The normal key's are basically extra persuading and speedier than uneven [2-5].

II. LITERATURE SURVEY

Cryptography is gotten from Greek "crypto’s", which means covered up or mystery and "graphein" signifies composing. It is the act of mystery composing utilized to share classified data over open systems, where substance of unique message are transformed into middle structure, so as

Revised Manuscript Received on July 10, 2019.

Gajula Lakshminarayana, Ph.D. Scholar, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Churela, Rajasthan-333001.

Dr. Anupama A. Deshpande, Professor, Dept. of EEE, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Churela, Rajasthan-333001.

Dr. Moparthy Gurunadha Babu, Professor & Dean, Dept. of ECE, CMR Institute of Technology, Hyderabad.

to be recovered just by the planned individual. Cryptography was being utilized in antiquated Egypt since 1900, where various symbolic representations had been cut for the motivation behind fascinating and beguilement.

Cryptography was first utilized as a mystery method for correspondence by Julius Ceaser from 100 to 40 century to hide important data, and his figure become the establishing stone of present day cryptography and is eluded as "Ceaser Cipher", where each character of the Roman letters in order is moved by three positions to one side. This move makes it jabber to the enemies. Prior encryption plans were extremely straightforward and consolidate the basic numerical tasks to change over a plain content to figure content. These methods were very helpless to recurrence fault. Since the origin of World War I, cryptographic calculations become increasingly mind boggling with the section of every day, as they were widely utilized in the transmission of classified data. Further, the usage of PC frameworks has altered the field of security as present day strategies to perform encryption and decoding at amazingly rapid bit level. Also, contemporary cryptography depends on certain numerical conditions which are practically difficult to explain until some uncommon criteria is met, these properties make it hard and arduous for an enemy to think of an fault.

Various components of the model are portrayed beneath:

- Plain content is the private data that will be encoded and sent over the system.
- Cipher content is the private data that has been scrambled utilizing an encryption calculation on the plain content.
- Encryption calculation is a method of complex numerical capacities which are utilized to scramble the secret data.
- Decryption calculation is likewise a mix of complex scientific capacities which are utilized to decode the private data. Normally an unscrambling calculation is an opposite of encryption calculation.
- Encryption key is a mystery esteems that the sender uses as one of the contributions to the encryption calculation related to plain content to produce a figure content.
- Decryption key is a mystery esteem that the collector utilizes as one of the contributions to the unscrambling calculation in synchronicity with figure content to get plain content.
- An fault is an element which dependably attempts to the communication channel to block the figure message and further endeavors to change over the figure content to plain content.

Cryptanalysis manages the investigation and examination of cryptographic calculations in a down to earth approach to comprehend their working and discover the vulnerabilities to break them. Cryptanalysis is used by military and some reconnaissance activities subsidized by huge associations so as to test security basic frameworks. In addition, programmers additionally use cryptanalysis to misuse vulnerabilities in various frameworks and sites. The way toward performing cryptanalysis isn't that basic, but it requires mastery in the field of science and inside and out understanding. In the old occasions, cryptanalysis was just intended to provide the key. This key will decode a message by contemporary cryptography. In this cryptography arithmetic and rapid PCs will break an encryption calculation.

Dlaminia et al, has introduced new developments in data security by using computers. Here the data security will have negative effect which will break the clients beneficent and financial development. Generally, anybody can communicate through computer and can use duplicate message for transmit and receiving. Classified information can be the subject of control and abuse. Since secure correspondence channel is hard to accomplish or there is insignificant dependence of system wide administrations, an assortment of safety efforts are expected to protect the information. Encryption is any type of coding, figuring, or mystery composing, and a pragmatic way to accomplish data mystery to guarantee its respectability amid transmission and away. Today, smart cards have been utilized in different applications and are getting to be common for installment components (for example pay TV get to control, transport, general store, banks, cashless candy machines), sending individual data (for example wellbeing cards, government ID cards), and for security get to (for example confirmation and controlled access to assets).

Here public key and private keys are allotted to both the sender and receiver. Every sender and receiver has one public key and one private key. The sender and receiver are figured out how to make a mystery key. This implies anybody may scramble (change of clear content to figure message) a message for a utilizing his open key. However by using ‘A’ we can unscramble (transformation of figure content to clear content) the message utilizing his mystery key and just we can encode the message that will decode with public key. As per, an information that traverses an unbound channel is vulnerable for recovery, and planned adjustment. Crooks use innovation to take personalities and submit extortion. An issue defying security in an open system incorporates how to distinguish the individual making the exchange, regardless of whether the exchange has been changed during transmission, or how to defend the exchange from being diverted or read to some other goal.

When we talk about "Smart Grids" from a client's viewpoint, somebody will consider gadgets that trade information to satisfy the requests of a client or to diminish vitality utilization. For example, a clothes washer decides the least expensive day by day vitality rate from the Internet to do the clothing. Actually, Smart Grids bear substantially more than basically contraptions that speak with every other to diminish costs. From the point of view of the vitality maker, the development of the overall vitality arranges likewise present new difficulties and security dangers for makers just as for clients. With vitality age frameworks like photovoltaics on rooftops, the maker/purchaser worldview in the field of power shifts. A portion of this so delivered power may surpass the required measure of vitality for warming a house. In this way vitality could be reused in the power lattice for different purchasers.

Vitality makers need to conform these progressions and attest the utilization of the shoppers and again than with customary metering approaches.

III. RELATED WORK

Security plays major role in present generation. There are a few encryption plans and every one of them is exceptionally relentless for some one of a kind application(s). As we discussed earlier that cryptographically hash work doesn't uses any key to secure the data. So master key encryption is used for protection and privacy. Basically, sender can keep key for every message in a session to encode it. This process is done only in crossover encryption. In crossover encryption, the sender can produce a session. For client verification public key cryptography is used. This public key cryptography will check whether the message is encrypted or not. If the message is not encrypted then it does not send the message to one client to another client. Security strikes be part of modification of messages or reports, refusal of organization, traffic examination and unapproved scrutinizing of a message of record. Computer contamination may be a champion among the foremost uncovered styles of ambush on info systems [12].

An amazing framework security methodology needs conspicuous proof of perils and at that time choosing the most effective game set up of instruments to overcome them. Security key schedule consists of diversifying round key to obtain new key. The enlargement of the accessibility of PCs makes various ways for shielding knowledge and messages from adjusting and scrutinizing. Gatecrashers could reveal the data to a private or affiliation use it to dispatch a strike or alter it to twist. So the intruders are productive to take risk for protecting the data. To hold the data first one should have to verify the system structure obtained in it. Likewise, one response for this issue is by mistreatment cryptography. Cryptography ensures that the messages could not be gotten or scrutinized by anyone apart from the supported recipient. It shields interlopers from having the power to use the data which will be secured.

At first cryptography protects its data in accustomed manner and by giving validity command. In this processed world, (information streams) assume the communication among PCs and systems. Moreover, an advanced info will usually thought as quite double info licitly. By using advanced info, we are able to usually get them organized to a few sorts: open data, like on-line papers and payer driven organization knowledge, that are obtainable to everybody; non-public info, like, the individual on-line collections and therefore the individual websites, that are shared within a bit gathering of individuals; and mystery info, as an example, military databases, therapeutic records, and sorted on-line archives, that are obtainable simply by approved purchasers. On these lines, the passion of knowledge security is high and increasing apace.

Private key cryptography or open key cryptography is employed to require care of the problem of key circulation. In lopsided keys, 2 keys are utilized; non-public and open keys. Open secret is utilised for cryptography and personal secret is utilised for unscrambling (E.g. RSA and Digital Signatures). Between the 2 varieties of cryptography systems, the parallel key cryptography is fast and most ordinarily utilised contrasted with the topsy-turvy key cryptography. Just in case of parallel key cryptography solely a solitary secret is used on the alternative sides of cryptography and unraveling. So by this parallel key, we can improve the speed by controlling sub bytes and columns. One such programming technique, known as the T-Box calculation, solidifies Sub Bytes and blend Columns in cryptography and Inverse Sub Bytes and Inverse combine Columns in decryption [6-8].

Generally, in today's generation, cryptography plays important role. This cryptography consists of plain text, cipher text which is very important to transmit message. Here encryption process is done only when plain text is transferred into cipher text. After this encryption decryption process is performed. so there are some requirements for cryptography which are given below:

1) Confidentiality: there should be confidentiality in the process while encrypting and decrypting a message.
2) Integrity: it should maintain good communication between sender and receiver.
3) Non-repudiation: it should delay the message while transmitting from sender to receiver.
4) Authentication: there should be an indication after receiving information from both senders to receiver.

IV. ADVANCED ENCRYPTION STANDARD STRUCTURE (AES)

For secure communications, cryptography is mainly used. the elements used in cryptography are plain text, key and cipher text. Coming to plain text, it is in the form of natural format. Cryptography is a practice and study of techniques for secure communication. The main intent of this plain text is to control the behavior of system. Next is cipher text, where the data is data is unreadable by the recipients. However the cryptography consists of symmetric key and asymmetric algorithms. Coming to symmetric key algorithm, it consists of same key for both encryption and decryption unit. The encryption unit uses the plain text and coming to decryption key, it consists of cipher text. Hence as generation increases the technology, the data encryption techniques also increases. Among those techniques mainly we use RC4 (Rivest Cipher 4), DES (Data Encryption Standard), AES and triple DES. Finally, here AES is nothing but advanced encryption standard, but it is also called as Rijndael cipher. This cipher is approved by the National Institute of Standards and Technology (NIST) of the United States in 2001 [1].

This advanced encryption standard (AES) consists of various key lengths; they are 64 and 128-bit. These all are belong to the symmetric key algorithm standard. Coming to block cipher which consists of two paired algorithms. Along with this two paired algorithms, it consists of encryption at sender side and decryption at receiver side. But here the AES algorithm shares the same key at sender and receiver side. Basically, in software platform there is no high speed data encryption.

Hence in real time applications, audio/video content encryption is used. This is about the software platform in encryption and decryption. Coming to the hardware implementation different architectures are used.

By using hardware architecture the area and power consumption is varied. Hence the optimization of hardware architecture is replaced by using conventional modules.

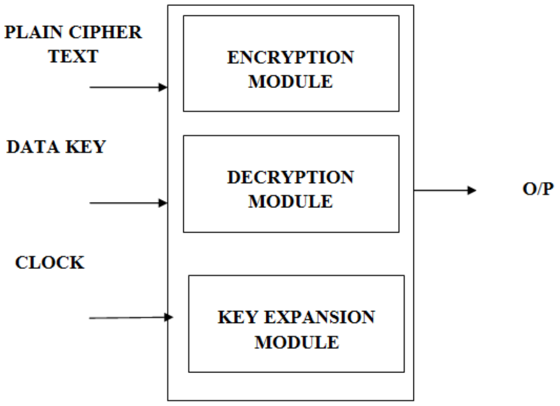


Fig. 2: Structure Of AES

The above figure (2) shows the architecture of AES system. In this three modules are used encryption module, decryption module and key expansion module. Here to encrypt the data, first input data and key are used. It process 128 bits in a key for every cycle. Now the encryption module will process the data as signal. Generally, before encrypting data, the existing system produces three control signals; they are clock, reset and go. Depend upon these three control signals the entire information will be encrypted and decrypted. Now the signal is encrypted then the clock will reset the position and transmit to the decryption module. The decryption module will use cipher text to control the decipher block. This decipher block consists of 128 bits.

Similarly, while decrypting the information, the AES system also takes three control signals and process will be continued. Transformation process is performed while decytimng the message, they are round key generation, sub byte transformation, substitution box. But here round key generation module is used to perform the operation. Because of inverse sub byte transformation, the look up table will change its value.

So, the AES (advanced encryption standard) takes four keys for further calculations which consist of 32 bits. It takes 32 bits for one round which of 44 words and in the same way second round takes 32 bits of 44 words. The process will be continued and the length of key is equal to 128 bits. So the duplicated key will holds the one expression which consists of 32 bytes. So at last 4 words will be obtained as pack of data. However the AES will not provide security in efficient way. So a new system is proposed which is discussed in below section.

V. ADVANCED SIMPLIFIED AES STRUCTURE (S-AES)

AES is a repetitive form. It depends upon 2 essential procedures to cipher and decipher knowledge known as substitution and permutation network (SPN).SPN is completely different from numerical exercises where the area unit is exhausted from square size computations. AES will manage 128 bits (16 bytes) as a hard and fast plaintext square size. These sixteen bytes area unit addressed in 4x4 framework and AES takes an endeavor at a cross section of bytes. The quantity of rounds is relied upon the length of key. To scramble and unscramble knowledge three key bits are used, for example, (64 & 128 bits). In this system mainly we use parallel prefix adder (PPA) and parallel prefix multiplier (PPM).

To perform the addition operation in high speed manner, we use mainly propagator and generator in parallel prefix adder (PPA). Basically, PPA is used for parallel sum of two multi-bit numbers. According to the adder's configuration, the prefix computation groups both values directly from the input. Based on the inputs given the outcome of operation is performed. As we know that the parallel prefix adder performs and executes the operation in parallel. The obtained output will be segmented into smaller pieces. There are different topologies used in parallel prefix adder, but the operator is associative. Based on topology the operation is performed. By using the associative binary operations, the algorithms will be generalized. This generalized algorithm performs certain operations and computed with particular efficiency. Basically there are two procedures followed in the system, they are in first pass the prefix sum as are calculated from the processing unit. And in second pass known prefix values are computed from processing unit to get initial value. So along with that the system performs two read operations and one write operation. Here a methodology is employed to design PPA. The experimental result mainly, depends on area, delay, and power consumption. The expense of additional area and remarkable will increase the power consumption. Compared with VLSI implementations, the Parallel-prefix adders will produce performance differently

While encryption process is performed, parallel prefix adder will generate the sum product by adding the upcoming signals. The obtained product is encrypted using encryption process. Next coming to decryption process, in this both parallel prefix adder and parallel prefix multiplier is used. These two combine to generate a final product and followed to perform the shift operation. The below figure (3) shows the structure of simplified AES.

A. Substitute Bytes Transformation

The main part of every spherical begins with Sub Bytes amendment. This stage depends on nonlinear S-box to substitute a computer memory unit within the state to a different computer memory unit. As shown by scattering and confusion Shannon's contents for scientific discipline estimation arrange it's basic employments to induce altogether bigger security. Substitution bytes transformation is compelled to provide security.

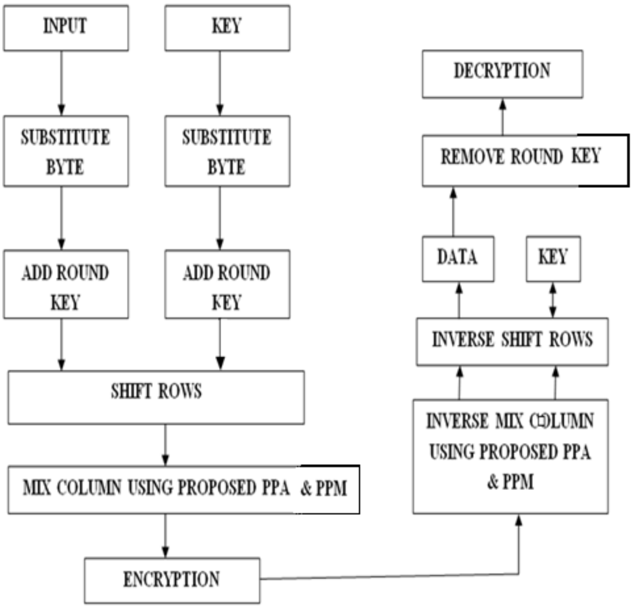


Fig. 3: Structure Of Simplified AES Structure (S-AES)

B. Shift Rows Transformation

After the sub byte transformation process, we follow the shift row transformation process. The shift row transformation will shift the bytes from one position to another position. Basically there are two positions right and left. In this, the byte is shifted towards left in each row. So after the transformation the shifted row remains zero and it does not carry any permutation. From figure we can observe that there are three rows commonly. Coming to first row only one byte is shifted circularly to left. In the same way in second row two bytes are shifted circularly to left. Lastly three bytes are shifted circularly to left. So from this we can observe that the size of new state will be remained same but their positions will be shifted according to state.

C. Mix Columns Transformation

After shift transformation we will follow the mix column transformation process. In this multiplication the each bytes play an important role. Here each byte in matrix transformation will multiply according to the column. Hence to obtain the bytes, the mix column uses XOR gate. So here the size of bytes will not hang but remains constant. Mix column transformation performs the operation of parallel prefix addition and parallel prefix multiplier. Coming to parallel prefix multiplier (PPM) it solves the problem of multi digit multiplication. The PPM is mainly depends on the property of distributive. In the same way the key component of PPM is partial products. Next the main intent of parallel prefix adder (PPA) is adding multi digit numbers.

D. Add Round Key Transformation

The most important key transformation in this proposed structure is Add round key transformation. Each key and information block measured in 4x4 network of bytes. The 128-piece key and information square measure distributed into the computer memory unit systems. Include spherical Key will provide significantly additional security amid scrambling data. This task depends on creating the association between the key and figure content. The figure content is originating from the past stage. The sub secret is incorporated by uniting every computer memory unit of the state with the relating computer memory unit of the sub key exploitation bitwise XOR.

AES count depends upon AES key augmentation to cipher and decrypt information. . Each round has a new key. AES algorithm is one of the most powerful algorithms that are widely used in different fields all over the world. This computation permits quicker than DES and 3DES counts to scramble and decipher information. Moreover, it's used in various cryptography conventions, for instance, Socket Security Layer (SSL) and Transport Security Layer convention to administer well additional interchanges security among client and server over the net.

VI. RESULTS

The below figure (4) shows the RTL schematic. RTL is abbreviated as register transfer logic. It flows the signals from hardware registers, and logical operations.

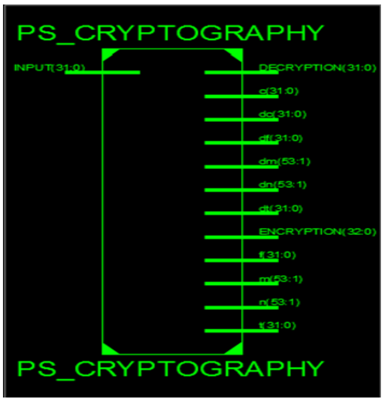
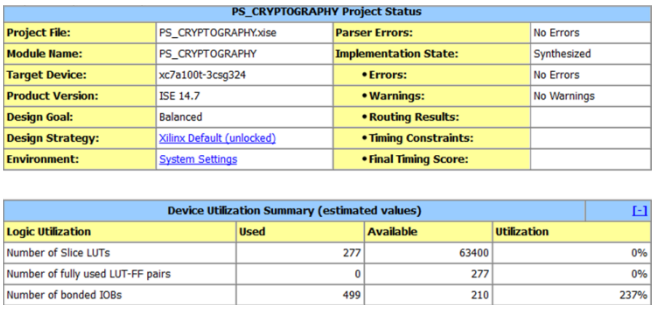


Fig. 4: RTL schematic

The below figure (5) shows the output report of usage of number of slides and boards in proposed system. Compared to existing system, proposed system gives effective results.



PS_CRYPTOGRAPHY Project Status			
Project File:	PS_CRYPTOGRAPHY.xise	**Parser Errors:**	No Errors
Module Name:	PS_CRYPTOGRAPHY	**Implementation State:**	Synthesized
Target Device:	xc7a100t-3csg324	• **Errors:**	No Errors
Product Version:	ISE 14.7	• **Warnings:**	No Warnings
Design Goal:	Balanced	• **Routing Results:**	
Design Strategy:	Xilinx Default (unlocked)	• **Timing Constraints:**	
Environment:	System Settings	• **Final Timing Score:**	

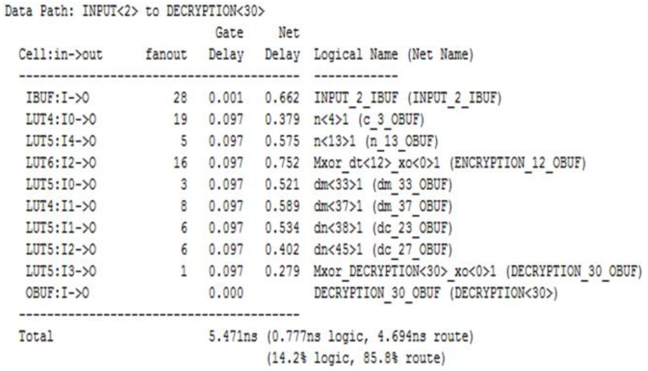
Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice LUTs	277	63400	0%
Number of fully used LUT-FF pairs	0	277	0%
Number of bonded IOBs	499	210	237%

Fig. 5: Final report

The below figure (6) shows the delay and memory usage of proposed system. In this total delay is 5.47ns, logic delay is 0.77ns and route delay is 4.694ns. The memory occupies 322300kbytes in proposed system.

Retrieval Number: I8989078919/19©BEIESP
DOI:10.35940/ijitee.I8989.078919

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



```
Data Path: INPUT<2> to DECRYPTION<30>
                                Gate     Net
  Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
  ----------------------------------------  ------------
   IBUF:I->O            28   0.001   0.662  INPUT_2_IBUF (INPUT_2_IBUF)
   LUT4:I0->O           19   0.097   0.379  n<4>1 (c_3_OBUF)
   LUT5:I4->O            5   0.097   0.575  n<13>1 (n_13_OBUF)
   LUT6:I2->O           16   0.097   0.752  Mxor_dt<12>_xo<0>1 (ENCRYPTION_12_OBUF)
   LUT5:I0->O            3   0.097   0.521  dm<33>1 (dm_33_OBUF)
   LUT4:I1->O            8   0.097   0.589  dm<37>1 (dm_37_OBUF)
   LUT5:I1->O            6   0.097   0.534  dn<38>1 (dc_23_OBUF)
   LUT5:I2->O            6   0.097   0.402  dn<45>1 (dc_27_OBUF)
   LUT5:I3->O            1   0.097   0.279  Mxor_DECRYPTION<30>_xo<0>1 (DECRYPTION_30_OBUF)
   OBUF:I->O                 0.000          DECRYPTION_30_OBUF (DECRYPTION<30>)
  ----------------------------------------
  Total                      5.471ns (0.777ns logic, 4.694ns route)
                                     (14.2% logic, 85.8% route)
```

Fig. 6: Delay and memory usage

The below table (1) shows the comparison between AES and S-AES. Here delay is reduced compared to existing system.

S.NO	PROPOSED SYSTEM	EXISTING SYSTEM
NO.OF.LUTS	277	366
NO.OF.IOBS	499	671
TOTAL DELAY	5.47ns	6.98ns
ROUTE DELAY	0.77ns	0.9ns
LOGIC DELAY	4.69ns	6.01ns

The below figure (7 &c 8) shows the comparison graph of AES and proposed system.

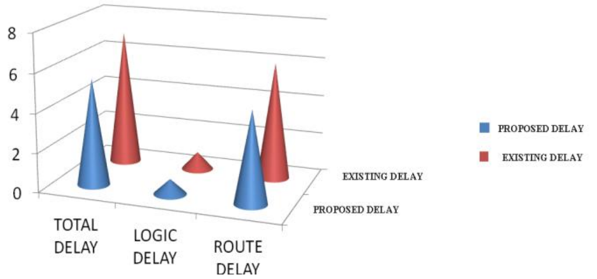


Fig. 7: comparison graph of delays

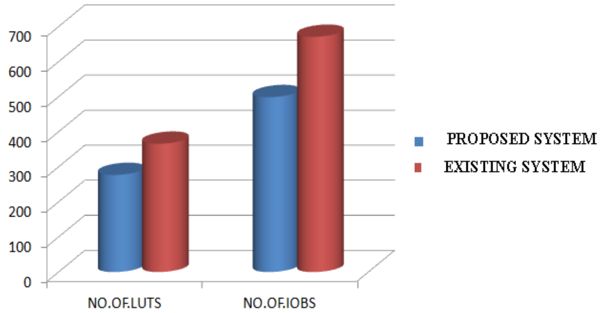


Fig. 8: comparison graph of LUTS and IOBS

VII. CONCLUSION

Both internet and system are increasing quickly. An excellent deal of advanced info is commercialism among clients. The main intent is to protect information from client. Secret writing calculations will protect the distinctive information from unauthorized client. Totally different kind of calculations area unit exist to write information. Simplified advanced encryption standard (S-AES) calculation is one in every of the productive calculation and it's generally transmitted and received on instrumentation and programming. In this paper, user will vary essential highlights of S-AES calculation and shows some past examines that have done to assess the execution of S-AES to scramble information using varied parameters. As per the outcomes got from inquires demonstrates that S-AES will offer well additional security contrasted with totally different calculations like DES, 3DES so forth.

REFERENCES

1. Mital Maheta "Design and simulation of AES algorithm Encryption using VHDL", International Journal of Engineering Development and Research Volume 2, Issue 1, 2014.
2. Hrushikesh S. Deshpande, Kailash J. Karande, Altaaf O. Mulani "Efficient Implementation of AES Algorithm on FPGA", Progress In Science in Engineering Research Journal, 2014, ISSN 2347-6680pp.170-175.
3. Ashwini R. Tonde and Akshay P. Dhande "Implementation of Advanced Encryption Standard (AES) Algorithm Based on FPGA", International Journal of Current Engineering and Technology, Volume 4, No.2, April 2014.
4. Hassan Anwar, Masoud Daneshtalab, Masoumeh Ebrahimi, Juha Plosila, Hannu Tenhunen "FPGA Implementation of AES-based Crypto Processor", IEEE 2013.
5. Abhijith.P.S, Mallika Srivastava, Aparna Mishra, Manish Goswami, B.R.Singh "High Performance Hardware Implementation of AES Using Minimal Resources", International Conference on Intelligent Systems and Signal Processing (ISSP), IEEE 2013.
6. K. Soumya, G. Shyam Kishore "Design and Implementation of Rijndael Encryption Algorithm Based on FPGA", International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 9, September 2013, pp.120-127.
7. Manjesh.K.N, R K Karunavathi "Secured High throughput implementation of AES Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering 3(5), May - 2013, pp. 1193-1198.
8. Bin Liu, Bevan M. Bass,"Parallel AES Encryption Engines for Many-Core Processor Arrays", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 3 MARCH 2013.
9. Pakkiraiah. Chakali, madhu Kumar. Patnala "Design of high speed Brent - Kung based carry select adder" IJSCE, Volume-3, Issue-1, march 2013
10. Nimmi Gupta "Implementation of Optimized DES Encryption Algorithm up to 4 Round on Spartan 3", International Journal of Computer Technology and Electronics Engineering , Volume 2 , Issue 1,Jan 2012.
11. HaridimosT.Vergos, Member, IEEE and GiorgosDimitrakopoulos, Member, IEEE," On modulo 2^n+1 adder design"IEEE Trans on computers, vol.61, no.2, Feb 2012
12. Ohyoung Song, Jiho Kim "Compact Design of the Advanced Encryption Standard Algorithm for IEEE 802.15.4 Devices", Journal of Electrical Engineering & Technology, Vol. 6, No. 3, pp. 418-422,2011.
13. David h, k hoe, Chris Martinez and Sri Jyothsnavundavalli "Design and characterization of parallel prefix adders using FPGAs", Pages.168-172, march2011 IEEE.
14. K. Vitoroulis and A.J. Al-Khalili, "performance of parallel prefix adders implemented with FPGA technology," IEEE Northeast Workshop on circuits and systems, pp.498-501, Aug 2007.
15. V. Ionescu, I. Bostan, and L. Ionescu, "Systematic Design for Integrated Digital Circuit Structures," in IEEE Journal of Semiconductor Conference, Vol.2, pp. 467 – 470, 2004.

Retrieval Number: I8989078919/19©BEIESP
DOI:10.35940/ijitee.I8989.078919

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication