# Pipelining Architecture of AES Encryption and Key Generation with Search Based Memory

Subashri T[1], Arunachalam R[2], Gokul Vinoth Kumar B[3], Vaidehi V[4]

Department of Electronics, MIT Campus, Anna University, Chennai-44
tsubashri@annauniv.edu[1], bgokul1989@gmail.com[2], r_arun21@yahoo.co.in[3],
vaidehi@annauniv.edu[4]

## Abstract.

*A high speed security algorithm is always important for wired/wireless environment. The symmetric block cipher plays a major role in the bulk data encryption. One of the best existing symmetric security algorithms to provide data security is AES. AES has the advantage of being implemented in both hardware and software. Hardware implementation of the AES has the advantage of increased throughput and offers better security. Search based S-box architecture has been proposed in this paper to reduce the constraint in the hardware resources. The pipelined architecture of the AES algorithm is proposed in order to increase the throughput of the algorithm. Moreover the key schedule algorithm of the AES encryption is pipelined to get the speedup.*

## Keywords

AES pipelining, Key pipelining, Search Based Memory, VLSI.

## 1.Introduction

Network security has three major security goals: confidentiality, availability and message integration between senders and receivers . Many algorithms are available in each of these three goals of security. One of the frequently used security algorithm in block cipher is the AES algorithm [3]. High speed security decisions are important in order to support multimedia data transmission. VOIP needs fast security algorithm to guarantee Qos in real-time voice transmission [10],[11].

Pipelining is an approach to increase the throughput of AES encryption and decryption algorithm. Speed of AES encryption depends on the number of rounds and the key generation involved in the algorithm. AES uses its own key expansion algorithm. Pipelined AES encryption and key pipelining in AES algorithm can increase the throughput of the algorithm.

Like encryption and decryption module another important component of AES algorithm is its key expansion module. Both of encryption and decryption module depends mainly on this key expansion module. This key expansion algorithm is based on iterative looping architecture [3]. If the architecture for AES with basic iterative architecture and partial loop unrolling is compared, the loop unrolling increases the speed of rounds implementation than the single round implementation in AES key expansion algorithm [4].Speed called as encryption throughput is the primary optimization criteria. The large change of the throughput ratio can be explained by the use of block RAMs in AES implementations. Blocks RAMs are used for S-Box implementation. Depending upon the searching process on this block RAMs the speed of S-box substitution is done in one of the four modules of a round. This search based memory is applied to the S-box in AES rounds implementation [5].

DOI : 10.5121/vlsic.2010.1405

In general cost of an algorithm covers the computational efficiency and storage requirement for different implementations such as hardware, software or smart cards. And the algorithm should have implementation flexibility and simplicity [5].This paper proposes a novel scheme incorporating these characters in AES.

The performance of both AES Key generation and AES encryption methods are determined. Performance of the key generation methods depends upon the secrecy of a key. So a key needs to be random. Random keys can be generated using Liner Feedback Shift Register(LFSR).

In this paper, section 2 describes the introduction to the AES algorithm; section 3 describes the pipelining of the AES algorithm, section 4 describes the search based memory, section 5 describes the pipelining of the key scheduling algorithm, section 6 shows the comparison of the different synthesized hardware utilization and finally section 7 presents the conclusion.

## 2.AES (Advanced Encryption Standard)

The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each AES cipher has a 128-bit input block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide [1], [2], [5], [6]. The AES algorithm organizes the data block in a four-row and row-major ordered matrix. In both encryption and decryption, the AES algorithm uses a round function.
The step involved are given below

1. Key Expansion using Rijndael's key schedule
2. Initial Round
    - AddRoundKey
3. Round
    - Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    - Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
    - Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column
    - AddRoundKey—each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.
4. Final Round (no Mix Columns)
    - Sub Bytes
    - Shift Rows
    - AddRoundKey

This is the iterative looping architecture of the AES. VERILOG code is written for the AES encryption algorithm for finding cipher for any given plaintext input. The next section describes the pipelining of the AES algorithm.

## 3.Pipelining of AES Encryption

As it can be seen from the figure 1 the pipelined architecture is just a modification of the iterative looping architecture except that in between the two rounds a register is included. These registers help us in achieving the pipelining of the AES.

Basically pipelining means to process the data that is given as input in a continuous manner without having to wait for the current process to get over. This pipelining concept is seen in many processors. In the architecture in the figure 1 the registers are used to store the current output of the round that is being executed. Now instead of passing the output of each round to the next round directly we use a register which would act as a bypass or an internal register. Since the current rounds' value is stored in the register the next input to the current round can be given as soon as the current output is obtained. And the input to the next round is given from the register thus avoiding a direct contact between the two rounds. This is not possible in the iterative looping architecture because the next input can be given only when the whole round based processing is over since the same hardware is used over and again in the process of obtaining the cipher text. Thus, the pipelined architecture increases the speed of execution for obtaining the cipher text but at a cost of increased hardware. In the substitute bytes we use a look up table based S-box. This contributes for some of the hardware in the form of block RAMs. With the help of a search based look up table (LUT) we can reduce the hardware cost to a considerable extent. This is described in the next section.

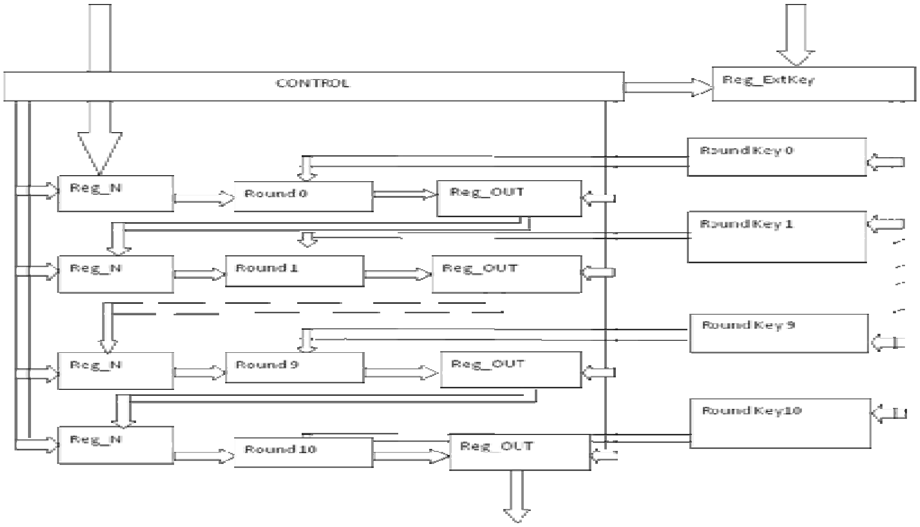


**Figure. 1.** Pipelining of AES encryption algorithm

From the results, it is very clear that, as the number of inputs is greater than 4 there will be progressive decrease in the time at which the output is obtained when compared to the AES iterative looping structure. Thus by using the AES pipelined architecture we have seen an increase in the throughput whose proportions increases as the size of data increases. Invariably, the size of inputs is going to be high in real time application as large volumes of data are fragmented in to 128 bits each and fed as input. But the hardware utilization is higher than that of the iterative looping architecture. But this is a trade off that needs to be done in order to achieve higher speeds in encryption.

## 4.Search Based Memory

It's a kind of storage technique which includes comparison logic with each bit of storage. A data value is broadcast to all words of storage and compared with the values there. Words which match are flagged in some way. Subsequent operations can then work on flagged words, e.g. read them out one at a time or write to certain bit positions in all of them. It is similar to a special type of computer memory used in certain very high speed searching applications.

Unlike standard computer memory (RAM) in which the user supplies a memory address and the RAM returns the data word stored at that address, this is designed such that the user supplies a data word and the algorithm searches its entire memory to see if that data word is stored anywhere in it. If the data word is found, the algorithm returns a list of one or more storage addresses where the word was found (and in some architecture, it also returns the data word or other associated pieces of data). This search based memory concept can be used in the S-box which results in the reduction of the number of block RAMs used thereby reducing the hardware utilization and making the pipelining more efficient.

## 5.Pipelining Of Key Schedule Algorithm

Apart from Encryption and Decryption Module, another main component is Key Expansion Schedule. The security factor of the AES Encryption / Decryption Standard mainly depends on this part. For better security, in AES Algorithm first round user key is XORed with the original Plain / Cipher Text. And next round onwards Expanded Key from Expanded Key Schedule is XORed with data. The expansion algorithm of the AES is fixed [5]. To speed up the process of Key Generation, it is preferable to opt for pipeline architecture

## 5.1.Pipelined architecture for key expansion module

The figure 2 presents the hardware architecture for Key Expansion Module which is one of the main components of the Grand Key. Key Expander comprises of EX-OR, Pipelined Data Registers. Since there are 44 words used in the key expansion process 44 data registers will be used, four in each stage of the pipeline.

From the figure 2 we can clearly see that registers are included between each round and thereby creating a sort of buffer between each round to provide the input without having to wait for the whole process to get over. So since the inputs are given at a faster rate and outputs are also obtained at a faster rate. So without pipelining the second output is obtained at the end of 22 cycles but with the help of pipelining the output is obtained at the end of 12 cycles thereby speeding up the process of obtaining the output.

## 6.Comparison of Hardware Utilization

As can be seen from the table 1, the hardware utilization of the pipelined architecture far exceeds that of the iterative architecture. But when a search based s-box is used in AES pipelined architecture some of the important device consumption are reduced or completely eliminated.

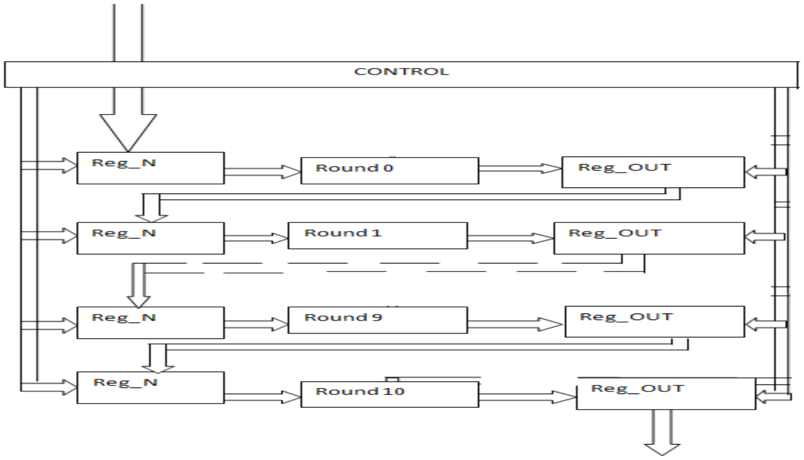
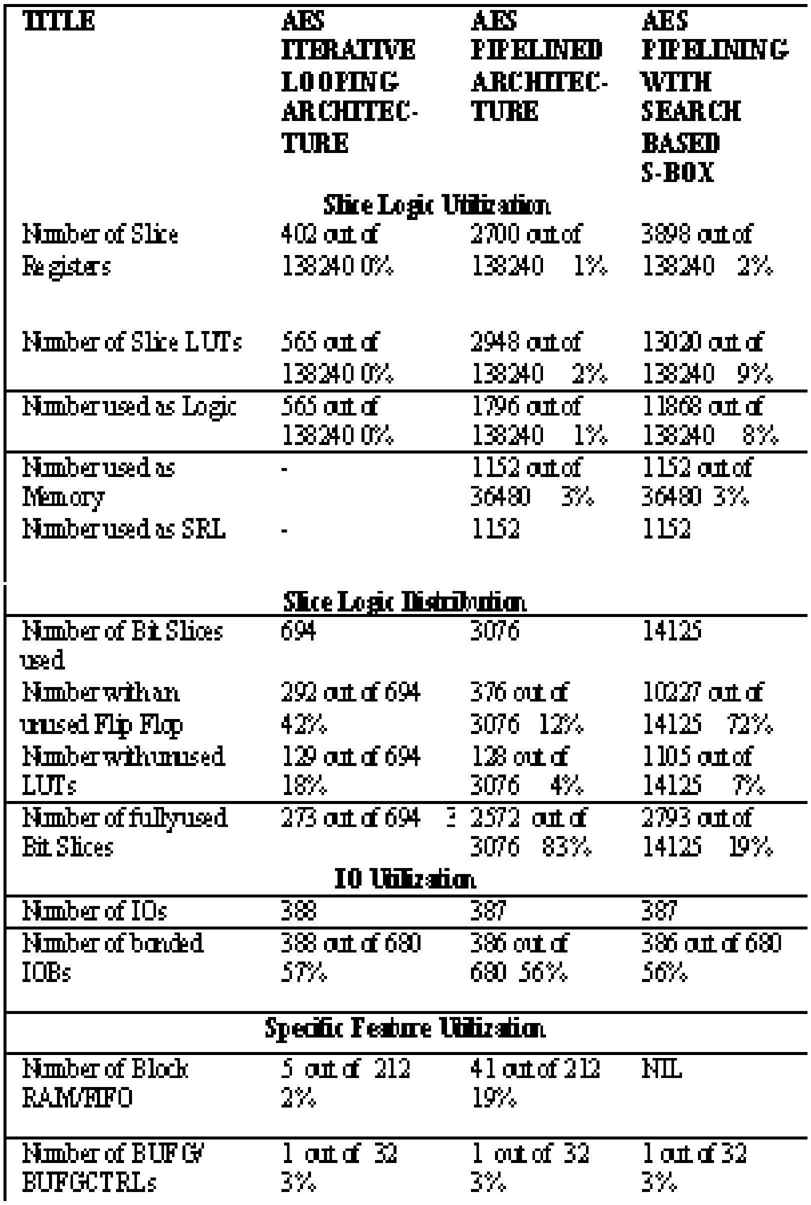


Figure. 2. Architecture of the pipelined key schedule algorithm

Features of the proposed method:

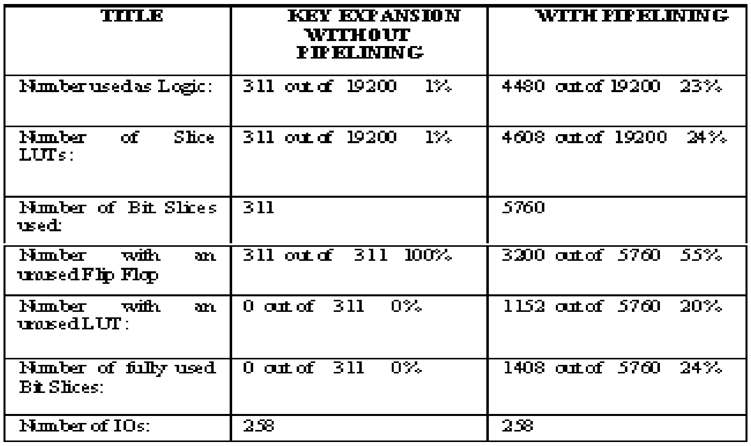
The need for Number of block RAMs which are important resources in any chips are completely eliminated when a search based S-box is used in AES pipelined algorithm. There is 2% consumption of block RAMs in iterative architecture without search based s-box and AES pipelined architecture on a virtex 5 board.[1],[2]. Also the Number of fully used Bit Slices is substantially reduced in *AES* pipelined architecture with a search based memory which is even lower than in the iterative architecture. The input/output device utilization is constant in all the three architectures. All other devices such as slice registers, flip-flops and LUTs are understandably lower in case of iterative architecture. Thus with the help of search based s-box in AES pipelined algorithm some of the key resource utilization is reduced. Trade-off between iterative architecture and pipelined architecture and at the same time ensuring the tremendous throughput as in pipelined feature[3].

The table 2 shows the comparison of the synthesized hardware utilization of the key expansion algorithm, with and without pipelining. It is clear from the table that the hardware utilized by the pipelined architecture is higher than th hardware utilized by the ordinary key expansion algorithm. There is a definite increase in the throughput. So there is a little trade-off that has to be made in the hardware utilization in order to get faster output.



| TITLE | AES ITERATIVE LOOPING ARCHITEC-TURE | AES PIPELINED ARCHITEC-TURE | AES PIPELINING WITH SEARCH BASED S-BOX |
|---|---|---|---|
| | **Slice Logic Utilization** | | |
| Number of Slice Registers | 402 out of 138240 0% | 2700 out of 138240 1% | 3898 out of 138240 2% |
| Number of Slice LUTs | 565 out of 138240 0% | 2948 out of 138240 2% | 13020 out of 138240 9% |
| Number used as Logic | 565 out of 138240 0% | 1796 out of 138240 1% | 11868 out of 138240 8% |
| Number used as Memory | - | 1152 out of 36480 3% | 1152 out of 36480 3% |
| Number used as SRL | - | 1152 | 1152 |
| | **Slice Logic Distribution** | | |
| Number of Bit Slices used | 694 | 3076 | 14125 |
| Number with an unused Flip Flop | 292 out of 694 42% | 376 out of 3076 12% | 10227 out of 14125 72% |
| Number with unused LUTs | 129 out of 694 18% | 128 out of 3076 4% | 1105 out of 14125 7% |
| Number of fullyused Bit Slices | 273 out of 694 | 2572 out of 3076 83% | 2793 out of 14125 19% |
| | **IO Utilization** | | |
| Number of IOs | 388 | 387 | 387 |
| Number of bonded IOBs | 388 out of 680 57% | 386 out of 680 56% | 386 out of 680 56% |
| | **Specific Feature Utilization** | | |
| Number of Block RAM/FIFO | 5 out of 212 2% | 41 out of 212 19% | NIL |
| Number of BUFG/ BUFGCTRLs | 1 out of 32 3% | 1 out of 32 3% | 1 out of 32 3% |

**Table 1.** Comparison of synthesized hardware utilization of different architectures of the AES algorithm.



| TITLE | KEY EXPANSION WITHOUT PIPELINING | WITH PIPELINING |
|---|---|---|
| Number used as Logic: | 311 out of 19200 1% | 4480 out of 19200 23% |
| Number of Slice LUTs: | 311 out of 19200 1% | 4608 out of 19200 24% |
| Number of Bit Slices used: | 311 | 5760 |
| Number with an unused Flip Flop | 311 out of 311 100% | 3200 out of 5760 55% |
| Number with an unused LUT: | 0 out of 311 0% | 1152 out of 5760 20% |
| Number of fully used Bit Slices: | 0 out of 311 0% | 1408 out of 5760 24% |
| Number of IOs: | 258 | 258 |

**Table 2.** Comparison of synthesized hardware utilization of key expansion with and without pipelining

# 7. AES Algorithm hardware implementation methods

Various methods of AES algorithm hardware implementation are, non feed back mode of AES, pipelining of AES and pipelining of AES key in encryption, AES pipelining with search based memory of S–box implementation, and implementation of LFSR based key in AES algorithm. From these implementations of AES algorithm it is possible to select suitable method of AES algorithm to get high throughput support in real time applications. In the existing encryption method for voice in real time application uses AES encryption scheme[3] .It is necessary to increase the rate of encryption of information for real time application

There are several operating modes followed for hardware implementation of symmetric block ciphers. These modes can be divided into 2 main categories.

1) Non feed back mode- Electronic code book (ECB) and counter mode
2) Feed back mode – cipher block chaining mode (CBC), cipher feed back mode (CFB), output feed back mode (OFB).

Encryption of each subsequent block of data can be performed independently from processing other blocks in the non feedback mode. In detail all blocks are encrypted in parallel. It is not possible in the case of feedback mode. As result, all blocks must be encrypted sequentlially, with no capability for parallel processing. Non feedback modes are parts of the standardization of ATM networks. The interleaved CBC mode has a potential to offer security of feedback modes combined with the performance of non feedback modes. Both of these modes are likely to be considered by NIST for standardization as future AES operating modes, and they become part of other standardization.

An important parameter which describes the operation of the key scheduling unit is encryption/decryption key set up latency. This is defined as the amount of time necessary to begin encryption or decryption after providing the input key. Key setup latencies are important in applications where only several blocks of data are encrypted between two consecutive key changes[8]. This key set up latency may play a important role on widespread protocols such as IPSec and ATM with small sizes of packets. And consecutive packets are encrypted using different keys. This can be minimized in the approach of pipelining on AES architecture. If the key set up latency is only the fraction of the time needed to encrypt one block of data, the key is allowed to change randomly[8],[9]. If the key setup latency is several times bigger than the time necessary to encrypt a single block of data. As the result, switching to the new key either introduces an extra delay or requires an additional circuitry to store the internal keys at the time.

## 7.1 Performance analysis of hardware implementation of iterative looping based AES architecture, pipelining architecture of the AES, and pipelining architecture with search based memory on s box of AES algorithm are compared.

An important resource is the number of blocks in any chips are completely reduced to NIL when a search based S-box is applied over the pipelined architecture of the AES algorithm. The number of fully pipelined AES used bit slices is reduced substantially with the search based memory of s box in the pipelined architecture of AES. It is also observed that the input and output device utilization is understandably constant. Thus with the help of search based S-box some of the main resource utilization is reduced. And also it is observed about the search based S box is ensuring the tremendous throughput as in pipelined feature.

Figure 3 shows the comparison of the various methods of AES encryption module. It can be seen that the hardware utilization in the pipelined architecture is far higher than in the iterative looping architecture. But the number of block RAMs is reduced with the use of a search based S-box. So with the use of AES fully pipelined architecture the throughput has been increased tremendously. But there is an increase in the area because of use of the fully pipelined architecture. This is a trade off that has to be made to achieve high speeds. If the search based S-box is used in pipelined architecture AES some of the important device consumption are reduced or completely eliminated.

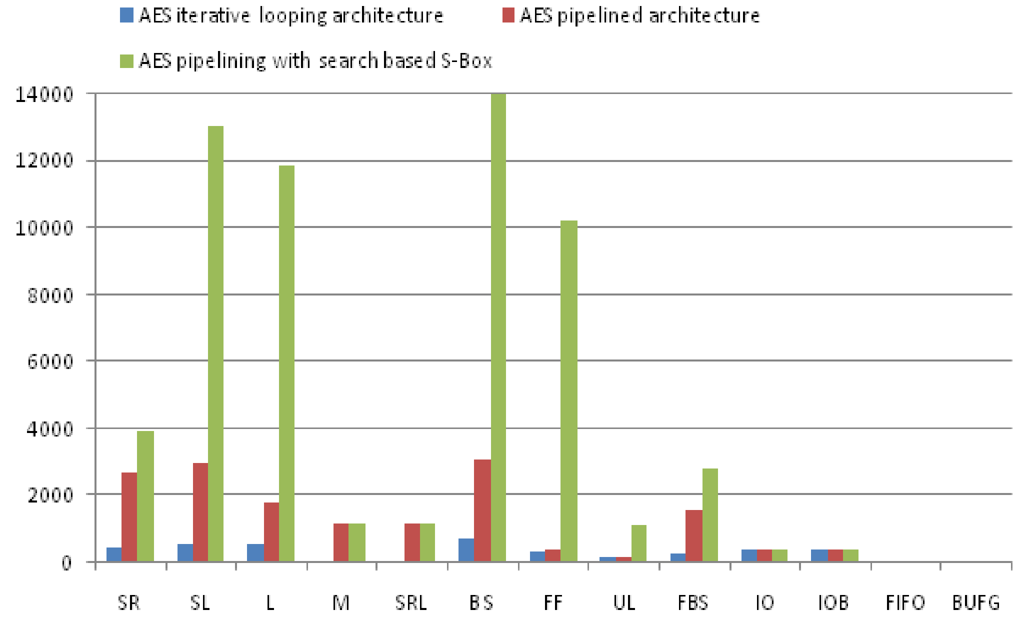


**Figure.3**. Performance analysis of iterative looping of AES algorithm, pipelined architecture, and search based S box on pipelined architecture of AES algorithm.

In this Figure 3 number of hardware measurement parameters is used to compare the AES implementation. By using three different architectures.SR is the number of Slice registers, SL is the number of Slice LUTs, L is the number used as logic, M is the number used as memory, SRL is the number used as SRL,BS is the number of bit slices used, FF is the number with an unused flip flop, UL is the number of unused LUTs, FBS is the number of full used Bit Slices, IO is the number of IO,IOB is the number of IOB,FIFO is the number of Block RAM/FIFO,BUFG is the number of BUFG/BUFGCTRLs.

## 7.2 Performance of the key expansion algorithm of AES encryption algorithm with pipelining and without pipelining.

The performance of the key expansion algorithm of AES algorithm is given in the figure 4 for without pipelining and with pipelining. Each round of AES algorithm needs round key from the key expansion algorithm. So the AES algorithm is also depends upon the speed of the round key generation. To increase the speed of key generation pipelining approach is used. The number of hardware utilization is compared with both pipelining key expansion algorithm and without key expansion algorithm.

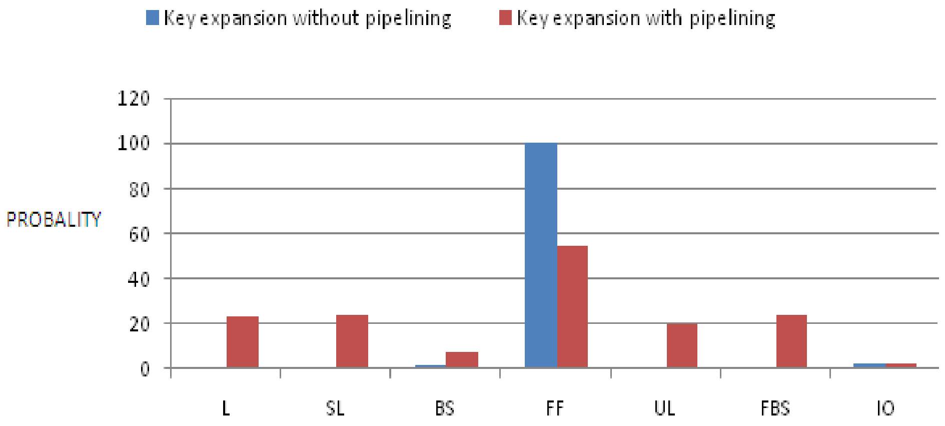


Figure.4. Performance of key expansion algorithm of AES encryption algorithm with pipelining and without pipelining.

## 7.3 Comparative analysis of computation time for various methods of AES key generation and AES encryption.

The comparison of time taken for various values in one round and 10 numbers of rounds are given in the figure 4 . Figure 5 presents comparison of time taken for various values of rounds involved in AES.X axis represents various modules of AES encryption algorithm and Y axis represents time in nano second Time taken for generating round key in AES algorithm using its own key expansion algorithm is compared with time taken for pipelined key generation of AES encryption algorithm. The time for one round key generation in key expansion and pipelined key expansion algorithm is 120 ns and 12 ns correspondingly. Time taken for AES encryption is 20 ns in AES encryption with pipelining and without pipelining. This can be reduced to 10 ns if the AES round uses search based S box substitution in module of the AES round.

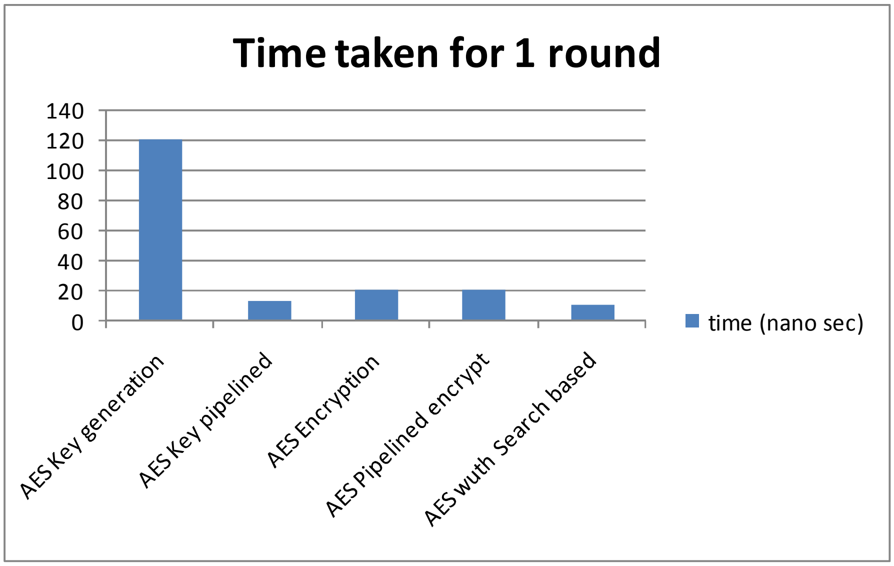


Figure.5. Comparison of time taken for various methods of AES key generation and AES

In the figure 6, shows timing analysis of various values of AES encryption and key generation of AES for 10 numbers of rounds. The time taken for 10 numbers of round key generations in AES algorithm is 1200 ns and it is higher than compared to 21 ns of pipelined method of AES generation. And the time for AES encryption and pipelined AES is compared in the analysis. They are correspondingly 200 ns and 29 ns for encryption. So the pipelined AES shows the reduction in the time consumption to encryption which can increase the speed of encryption and throughput of the encryption algorithm. In addition with the search based S-box on the pipelined AES reduces the number of hardware utilization. And also this search based S-box produces minimization of time in the searching process of S-box.

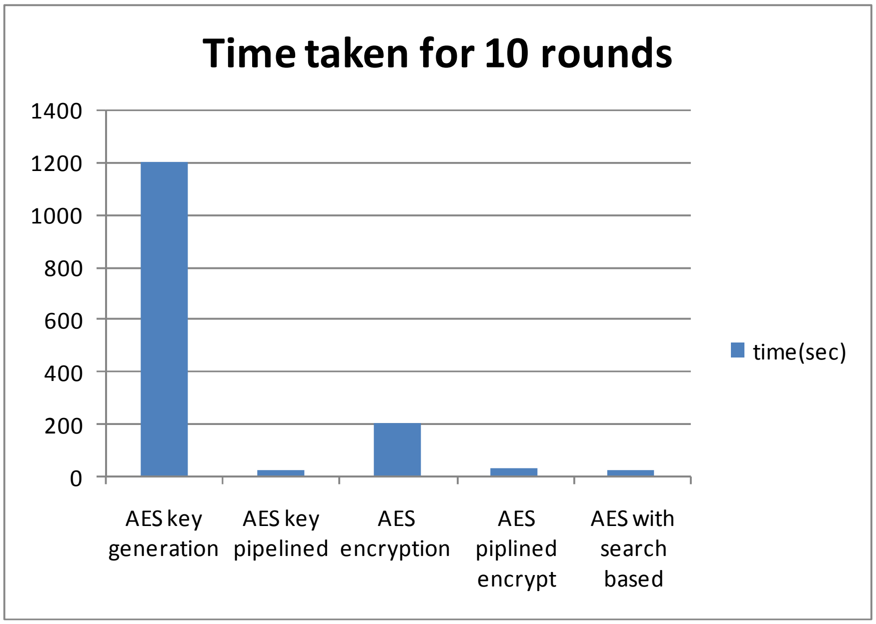


**Figure.6.** Comparison of time taken for various methods of AES key generation and AES

## 7.4 Comparison of hardware utilization of various methods of AES encryption methods.

Hardware utilization of different methods of AES encryption algorithm is given in the figure 7. Overall hardware utilization in the implementation of AES encryption is compared here. Pipelined AES algorithm requires 10% of additional hardware compared to the standard encryption algorithm. But this additional hardware requirement can be further reduced by using search based S-box in the pipelined AES encryption stages. The hardware utilization of pipelined AES encryption and pipelined key generation is provided  in the figure 6. The hardware utilization of the LFSR based key performance on AES encryption algorithm and counter mode of AES encryption algorithm is also provided. In this implementation, counter mode of AES encryption algorithm can use the same hardware present in standard AES algorithm. The non feedback method of AES encryption is a counter mode which uses the same hardware for decryption. Thus the number of hardware used for the AES algorithm is reduced. This can be used in VoIP environment for better support with minimum number of hardware. The information rate obtained by AES encryption algorithm exceeds with an average of 4.3 compared to the standard encryption algorithm. In VoIP network the speed of throughput of the confidential information can be increased by using the search based S box on pipelined AES using minimum number of hardware. The encryption algorithm aims at two constraints; one is to increase the speed of the Information rate and the other is lesser number of hardware.

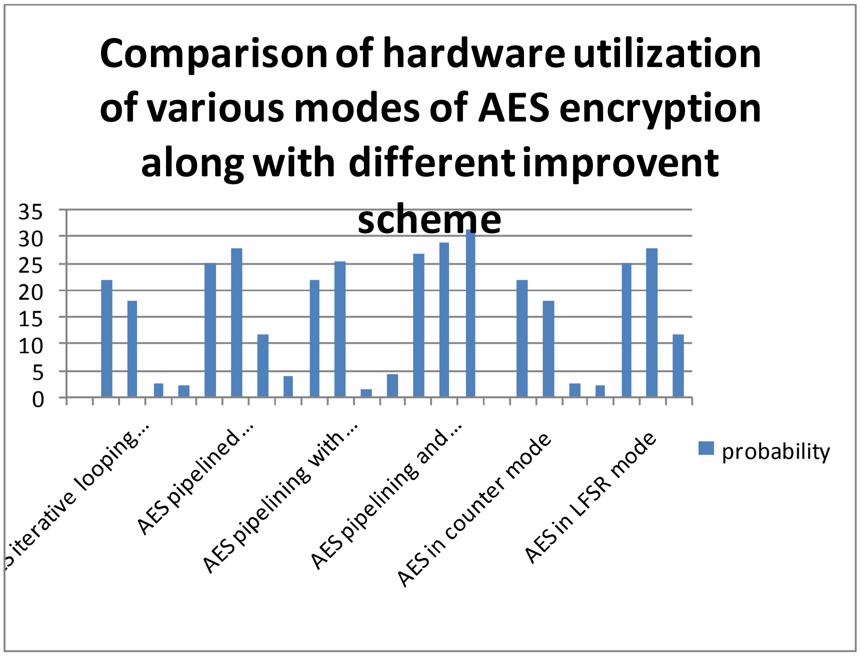


**Figure.7**.Comparison of hardware utilization of various methods of AES encryption.

## 8. Conclusion

The speed of encryption is of prime importance in applications where data is to be transmitted at high speeds. Thus, with use of fully pipelined architecture the throughput and hence the speed of encryption is increased tremendously. But there is an increase in area because of pipelining. In an attempt to reduce this area search based S-box was implemented and this was successful in reducing the number of block RAMs. The hardware implementation provides faster speed and better security when compared to software models. Thus the proposed method could be successfully implemented in currently developing technologies like VoIP systems where encryption of both voice and data takes place and where the speed of encryption is very critical. Also a pipelined architecture of the key pipelining was proposed which can be utilized in the environment where the key needs to be changed at a faster rate.

LFSR based key can also be a solution for the requirement of faster key rate needs certain in environment. Counter mode of AES encryption algorithm is also implemented through this proposal. This non feedback counter mode does not depend on additional hardware for decryption which uses the same amount of hardware VoIP environment.

# REFERENCES

1. J. Elbirt, W. Yip, B. Chetwynd and C. Paar, “An FPGA Implementation and Performance evaluation of the AES Block Cipher Candidate Algorithm Finalist, “The third AES Conference (AES3), New York, Apr. 2000. Available at http://csrc.nist.gov /encryption/aes/round2/conf3/aes3papers.html.
2. A. J. Elbirt, W. Yip, B. Chetwynd and C. Paar, “An FPGA Implementation and Performance evaluation of the AES Block Cipher Candidate Algorithm Finalist” IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 9, NO. 4, AUGUST 2001.
3. X. Zhang and K. K. Parhi, “Implementation Approaches for the Advanced Encryption Standard Algorithm,” IEEE Circuits and Systems Magazine, vol.2, Issue.4, pp. 24-46, Fourth Quarter 2002.
4. K. Gaj and P. Chodowiec, “Hardware performance of the AES finalists survey and analysis of results.” [Online]. Available citeseer.ist.psu.edu/460345.html
5. National Institute of Standards and Technology, Specification for the Advanced Encryption Standard (AES). FIPS PUB 197, available at http://csrc.nist.gov, 2001.
6. Kris Gaj, Pawel Chodowiec, “Comparison of the hardware performance of the AES candidates using reconfigurable hardware”, International conference on Advanced encryption standard candidate conference, April 13, 2000.
7. John Kelsey, Bruce schenier, “MARS attacks! Preliminary cryptanalysis of reduced round MARS variants”, Third international conference on advanced encryption standard candidate conference, 2000.
8. Lan Harvey, “The effects of multiple algorithms in the advanced encryption standard”, International Conference on advanced encryption conference, 2000.
9. FIPS (Federal information processing standards), “Advanced Encryption Standard”, issued by NIST, November 26, 2001.
10. D.Richard Kuhn, Thomas J. Walsh, Steffen Fries,“Security Considerations For Voice Over IP Systems”, NIST Special Publication, January 2005.
11. Feng Cao and Saadat Malik, “Vulnerability Analysis and Best Practices for Adopting IP Telephony in Critical Infrastructure Sectors”, IEEE Communications Magazine, pp138-145, April 2006.
12. Wiretapping Woes Upson.S, Spectrum, IEEE Volume 44, Issue 5, May 2007, Pages: 10 – 12.
13. William Stallings, Cryptography and Network Security- Principles and Practice, third edition, Pearson Education.
14. J. M. Rabaey. Digital Integrated Circuits. Prentice Hall, 1996.

## Authors

V. Vaidehi received her B.E. in Electronics and Communication Engineering from College of Engineering, Guindy, M.E. in Applied Electronics and Ph.D. from Madras Institute of Technology, Chennai. She was a recipient of academic exchange fellowship of Association of Common wealth Universities. She has carried out funded projects on Tracking Algorithm for ship borne RADARS — funded by LRDE; GPS signal simulator — funded by Ministry of Information Technology; University Micro satellite — funded by ISRO; Semantic Intrusion Detection System — funded by Xambala Inc. Multi Sensor Data and Image Fusion, Power optimization in Wireless Sensor Network-funded by TCS. Currently she is a Professor and Head of Department of Information Technology, Madras Institute of Technology, Chennai. Her areas of interests are Networking, Parallel processing and Embedded systems.

Ms.T.Subashri received her B.E in Electronics and Communication Engineering from Thiayagarajar College of Engineering, Madurai, M.E in Communication Systems from Thiayagarajar College of Engineering, Kamaraj University, Madurai. Her areas of interests are Networking, cryptography & Network Security, Communication Systems. Currently she is persuing her PhD from Anna University.