SECURITY ENHANCEMENT OF INFORMATION USING MULTILAYERED CRYPTOGRAPHIC ALGORITHM

Lakma Kalyan[1] , Dr S Kishore Reddy[2] , Jaldi Merina[3] and P Vijnatha Raju[4]

[1]M.Tech Student, ECE, VLSI System Design, Avanthi Institute of Engg. & Tech., Hyderabad, India.

[2]Associate Professor, HOD, ECE, VLSI System Design, Avanthi Institute of Engg. & Tech., India.

[3]Assistant Professor, ECE, VLSI System Design, Avanthi Institute of Engg. & Tech., Hyderabad, India.

[4]Assistant Professor, ECE, VLSI System Design, Avanthi Institute of Engg. & Tech., Hyderabad, India.

Abstract - *In response to the rising concern for the safety of data while it is being sent across computer networks, a number of different types of encryption solutions have came into being. An encryption standard known as the AES was developed by the National Institute of Standards and Technology (NIST) ensure the safety of data encrypted electronically. The definition that is provided in the previous publication, FIPS Publication 197, is in accordance with the Federal Information Processing Standards standards. encrypt and decode 128-bit blocks, the AES employs cipher keys that are 128 bits wide (AES128). This may be accomplished successfully.Within the scope of this investigation, the AES128 encryption algorithm was proposed as a potential hardware implementation strategy. By virtue of the fact that it creates the round keys at the same time as the encryption, the pipelined solution that was presented stands out as particularly noteworthy, do several rounds of encryption, these round keys are used. The overall amount of time required to encrypt a plaintext block as well as the amount of time that passes between encryption rounds are both significantly reduced as a result of this consideration. As a consequence of this, the throughput of message encryption is increased as a result.*

Keywords – *AES, Encryption, AES128, Cryptographic, Multilayered.*

I. INTRODUCTION

When it comes to encryption standards, the United States Federal Information Processing Standard (FIPS) 192, which was published in November 2001, establishes AES, which is an acronym for "Advanced Encryption Standard," as the standard. It received the status of a federal standard in May of 2002. The most current algorithm that the federal government of the United States of America has allowed for use is the AES. It would be inappropriate to compare the AES to RSA, which is another prominent algorithm, since RSA is a member of a different category of algorithms. It is not common practice to encrypt large amounts of data while using RSA.RSA is useful in a number of contexts, including digital signatures and the transfer of extra encryption keys (such those used by AES), to name just two instances. symmetrically encode data, the AESmakes use of blocks that are 128 bits in size. The difference between bits and decimal digits is that bits are functionally binary digits, which have two possible values: zero and one. Decimal digits, on the other hand, may take any one of 10 distinct values. A key is

used to transform a block of 128 bits into a new block of the same size in a manner that is distinct. This is done encrypt the block. AES is considered to be symmetric it uses the same key to both encrypt and decode data. It is just necessary to keep the key a secret guarantee safety. An example of how AESmight be configured to use different key lengths is provided by the three key lengths that are defined by the standard: AES-128, AES-192, and AES-256. Adding extra bits to the key makes it twice as difficult for an attacker to launch a brute force attack, which entails attempting every possible combination of keys until they find the right one. There is a direct proportional relationship between the amount of bits in the key and the strength of the approach.

A. A brief overview of AES

The DES, which had been around for quite some time, was in need of replacement when the National Institute of Standards and Technology of the United States released a call for ideas in the year 1997. After a process that was completely open to the public and three international conferences that were also open to the public, the number of applications was reduced from fifteen to five. February 2001 was the month that saw both the announcement of the final candidate and the accompanying call for input. Twenty-one different organizations and individuals contributed their thoughts and opinions. There was not a single concern about the algorithm that was being offered. The AES seems to be effective against all known attacks, because it is based on mathematics that has been well documented and is solid. Given that it has been available for some time, that it has been subjected to rigorous testing by researchers all around the globe, and that it is already safeguarding such enormous amounts of data and economic value, there is solid reason to think that there is no known weakness or backdoor. there are no unknown components in its formation, the conspiracy charges that have been thrown against an encryption standard that was developed by a government agency in the United States have been laid to rest as a result of its development by expertise from Belgium. • Brute force, also known as testing every possible key until one works, is the sole method that can be used to find the unencrypted plain text in the event that the key is unknown. This is the one major condition that a successful encryption method must meet.

B. Encryption must be done properly :

The AES may be implemented in a number of different ways, just like any other algorithm. Certain strategies are effective when used in certain situations. Even while AES is secure in and of itself, the output may not be secure if the appropriate method is not adopted in each and every instance. The AES is a straightforward encryption method; nevertheless, use it appropriately for a particular situation, a significant amount of experience and understanding is required. In the same way that a set of tools may turn someone into a proficient carpenter, AEScannot make a system safe on its own. Unfortunately, there is not enough space in this short introduction to go into depth on the precise methods in which AES may be used for a variety of applications.

C. Strong keys :

It is possible for an encryption key that is based on AES to have a length of 128 bits, 192 bits, or 256 bits. The use of strong and outstanding keys is just as vital as the right use of AES, given that the security provided by AES is rendered ineffective if the key is easy to guess. Using a computer to produce one good and strong key is an unexpectedly difficult task that requires careful preparation. This challenge is a problem that requires careful planning. A good and strong key needs randomness and unpredictability, which is difficult to accomplish with

computers due to their notorious determinism. This is because computers want to be as predictable as possible. It is very improbable that the length of keys created from human-entered passwords or passphrases exceeds 128 bits, much alone 256 bits, when they are used in conjunction with an encryption technique. To accomplish the goal of achieving 128-bit equivalence in a pass phrase, it is necessary to have a minimum of 10 conventional passwords, such as those that are used in an ordinary work environment. Special techniques have the potential to significantly strengthen weak keys by increasing the amount of effort required to break them. This is accomplished by adding stages that are computationally expensive. There are risks associated with inappropriate usage, implementation, and weak keys that are present in any encryption scheme; AES is not an exception to this rule. The amount of security that is provided may be easily determined by providing a response to a basic inquiry about the actual number of bits that correspond to the key, password, or pass phrase. This is assuming that the implementation is done correctly. When the key is not generated by a true random generator, the computation of this estimate becomes a great deal more challenging.

II. ADVANCED ENCRYPTION STANDARD

A. Cryptography Protocol Version 2 (AES)

acts as a guidance for the protection of information stored in digital media. The broad acceptance of this practice around the world may be attributed to the United States government's decision to embrace it. Within the framework of the symmetric-key approach that is described by AES, both the encryption and decryption of data are carried out using the same key.

The AESwas officially designated as the United States Federal Information Processing Standard (FIPS) Publication 197 (FIPS 197) on November 26, 2001, after a standardization process that lasted for five years and involved fifteen competing designs. Please refer to the Advanced Encryption Standard method for more information. On the 26th of May in the year 2002, it became a standard for the federal government after receiving clearance from the Secretary of Commerce. It is possible to locate it in a number of different encryption schemes. (For further information, see the section below under "Security of AES") The NSA has given permission for AES, the first encryption that is accessible to the public, to be used to safeguard top-secret material.

Following the development of the cipher under the name Rijndael, the two Belgian cryptographers, Joan Daemen and Vincent Rijmen, first presented it to the selection process for the AES. The names of the two people who created the game are combined in an ironic way to get the name Rijndael.

AESis the name of the standard, and the approach that is being discussed is a (limited) variant of Rijndael. Despite this, the approach is sometimes referred to as "AES" in practice, which is an abbreviation that contains the phrase "a case of totum pro parte."

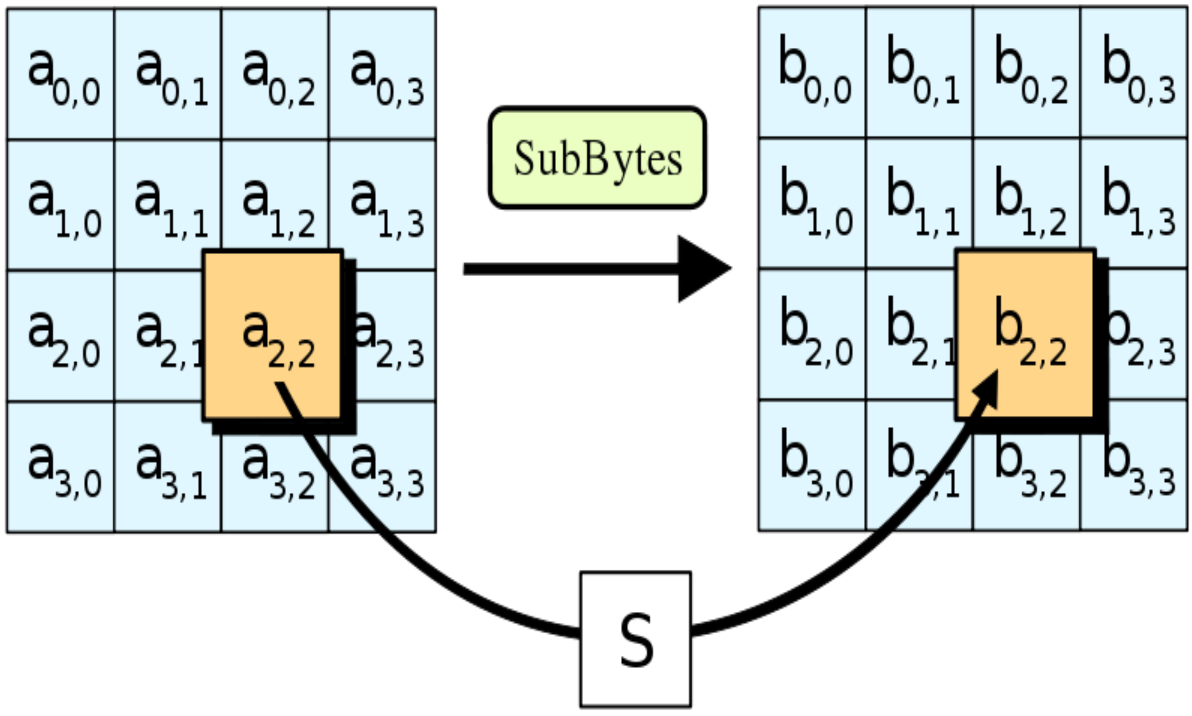
B. An explanation of the encryption

A method known as a substitution-permutation network serves as the basis for the AES. It is quite rapid in terms of both the technology and the software required.(6) [6] Unlike DES, AESdoes not depend on a Feistel network.

Rijndael allows for block and key sizes to be selected in any multiple of 32 bits, that is in contrast to the AES, which demands a minimum of 128 bits for blocks and a maximum of 256 bits for keys. When it comes to blocksize, there is a theoretical maximum limit of 256 bits; however, there is no such restriction for keysize.Versions of Rijndael that consist of larger block sizes have a bigger number of columns in the state, which is a 4×4 column-major order matrix of bytes that is used by the AES. When performing the majority of AES calculations, a specific finite field is used.

C. The process of SubBytes

When the SubBytes step is performed, each and every byte in the matrix is altered by using the Rijndael S-box, which is an 8-bit substitution box. This procedure is responsible for providing the non-linearity used in the cipher. An S-box that has outstanding non-linearity properties was selected; it is a product of the multiplicative inverse over GF(28). After integrating the inverse function with an invertible affine transformation, the S-box is constructed protect itself against attacks that are based on simple algebraic characteristics. In addition, the S-box has been chosen. In addition, the S-box is chosen steer clear of both fixed points (and hence derangements) and fixed points that are oriented in the opposite way.



D. Side-channel attacks:

Attacks that target machines that have the cipher implemented and unwittingly reveal data are known as side-channel attacks. These attacks do not compromise the security of the underlying encryption for any reason. It has been shown that some implementations of AES are susceptible to a number of attacks of this kind.

In April of 2005, D.J. Bernstein made the revelation of a cache-timing attack, which enabled him to get into a custom server that used OpenSSL's AESencryption.[23] [23] "The" For the attack, it was necessary to have more than 200 million examples of chosen plaintexts. Bernstein made the observation that even though the custom server was designed to supply a substantial amount of timing information (the server reports the number of machine cycles that were utilized by the encryption operation), "reducing the precision of the server's timestamps, or eliminating them from the server's responses, does not stop the attack: the client simply uses round-trip timings based on its local clock, and compensates for the increased noise by averaging over a larger number of samples."

E. NIST/CSEC validation:

During the operation of the Cryptographic Module Validation Program (CMVP), the Computer Security Division of the National Institute of Standards and Technology (NIST) in the United States and the Communications Security Establishment (CSE) of the Government of Canada work together to ensure that the program's integrity is maintained. On the other hand, the government of the United States does not mandate the use of recognized cryptography modules for applications that are not considered to be cryptographic. To add insult to injury, the government of Canada recommends that all departments use cryptography modules that have been approved by FIPS 140 for their applications that are not classified.

It is a regular practice for manufacturers to contact the CMVP under FIPS 140 and seek the simultaneous validation of other algorithms, such as Triple DES or SHA1. This is the case despite the fact that NIST publication 197, which is sometimes referred to as "FIPS 197," is the only document that makes mention to the AESmethod. As a result of the fact that the National Institute of Standards and Technology (NIST) does not regularly release FIPS 197 verified modules individually on its public website, cryptographic modules that are specifically validated by FIPS 197 are not very prevalent. In contrast, the current list of cryptographic modules that have been verified by FIPS 140 commonly includes FIPS 197 validation as "FIPS approved: AES" notation, which is accompanied by a particular FIPS 197 certificate number. This is because FIPS 140 is the certification body that validates cryptographic modules. According to the vast majority of cases, this is the situation.

III. AREA-OPTIMIZED AES-128

A. The Rijndael Algorithm: A Concise Overview

The unique characteristics of the Rijndael method may be attributed to its three components: key scheduling, encryption, and decryption. The Rijndael method is comprised of three basic components that are responsible for encrypting data. These components are the SubBytes operation, the ShiftRows operation, the MixColumns action, and the AddRoundKey instruction. Look at Figure 1 to understand what I mean.

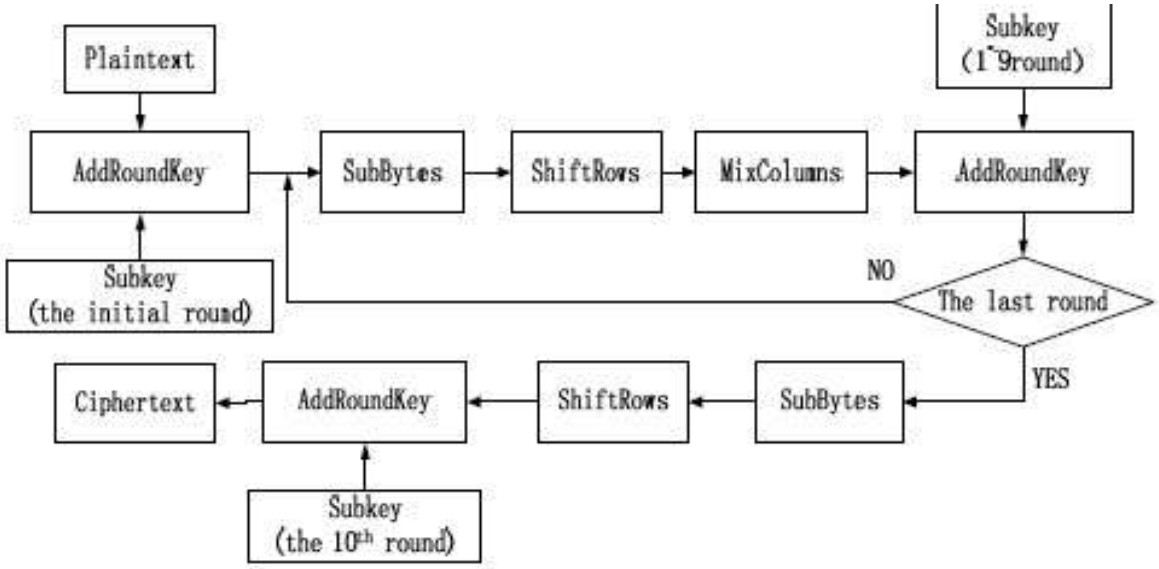


Figure 1. How the Rijndael algorithm for encryption is structured

The plaintext is used as input for an encryption method, which then applies the number one plus one to it generate the ciphertext. correspond to key lengths of 128, 192, or 256 bits, the AESalgorithm's Nr value should be 10, 12, or 14, respectively, for packets that are 128 bits in length. Only the Advanced Encryption Standard (AES-128), which is a type of encryption that uses keys with a length of 128 bits, is taken into consideration in this research.

B. A New and Better AES-128 Cryptography Method

1) **The Advanced Encryption Standard two primary procedures**

The algorithm known as the AESis comprised of two primary elements: the key schedule and the round transformation as its two primary components. The two components that comprise a key schedule are the selection of keys and the enlargement of certain keys. During the process of key expansion, which entails mapping Nk bits of the original key to it, the enlarged key module is used. On the other hand, the round key selection makes use of it choose Nb bits of the round key.

The four primary components that make up Round Transformation are the ByteSubstitution, ByteRotation, MixColumn, and AddRoundKey modules.

2) **Key points for the design**:

A 4×4 two-dimensional matrix is used to map the data in the primary procedure discussed earlier in the AES-128. The matrix, seen in Figure 2, is also known as the state matrix.

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

Figure 2. The state matrix

In the four transformation modules of round transformation, the ByteRotation, MixColumn and AddRoundKey are all linear transformations except the ByteSub.

It is important to take into consideration the bytes substitution action of the S-reversible box, which is both independent and uncomplicated. To get things started, the state matrix is comprised of four columns. do byte replacement, the next step is to make use of the look-up table, which can be seen in Figure 3.

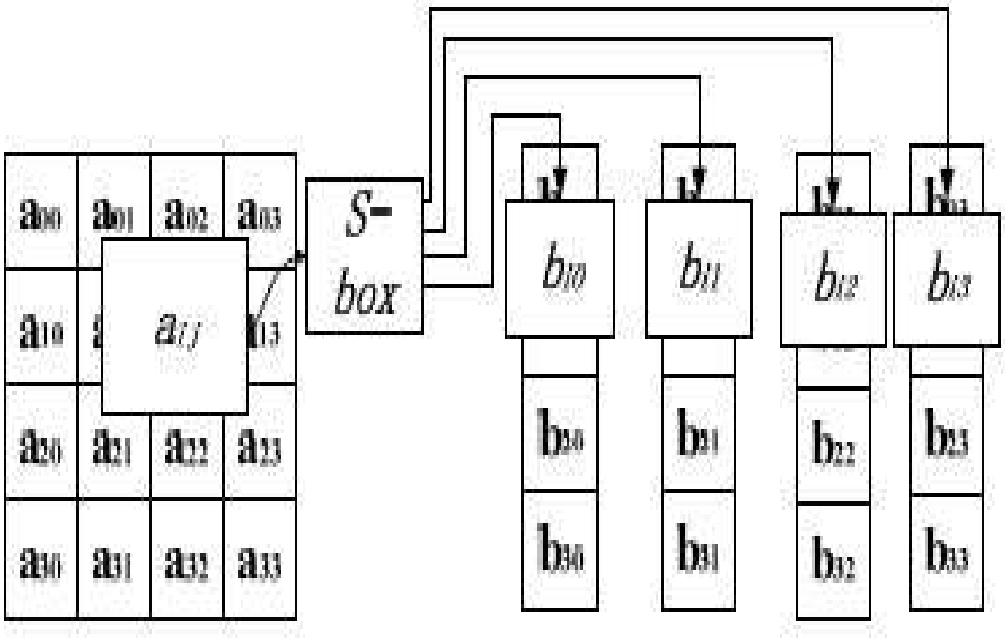


Figure 3. Segmenting bytes and processing replacements

In light of this, the plaintext and key will be generated using four consecutive 32-bit input sequences, rather than the 128-bit inputs that were initially developed. The number of output ports was decreased by using four

successive 32-bit ciphertext sequences rather than the previous 128-bit output, which needed a clock controller. This was done lower the number of output ports. Prior to the pipelining method, the 128-bit data is also partitioned into four sets of 32-bit data in the round transformation. This is done before the pipelining phase.

C. The Process of New algorithm

AES encryption is comprised of two fundamental components, which are the key schedule and the round transformation, as shown by the research that was presented before. In addition, the improved structure is separated by these two essential processes. Immediately after the selection of the roundkey, the initial key will be delivered to Keyexpansion and Keyselection, while the plaintext will be sent to the round transformation. This is in contrast to the data transfer operand, which is transformed into a 32-bit unit. Fig. 4 provides a visual representation of the enhanced algorithm in action.

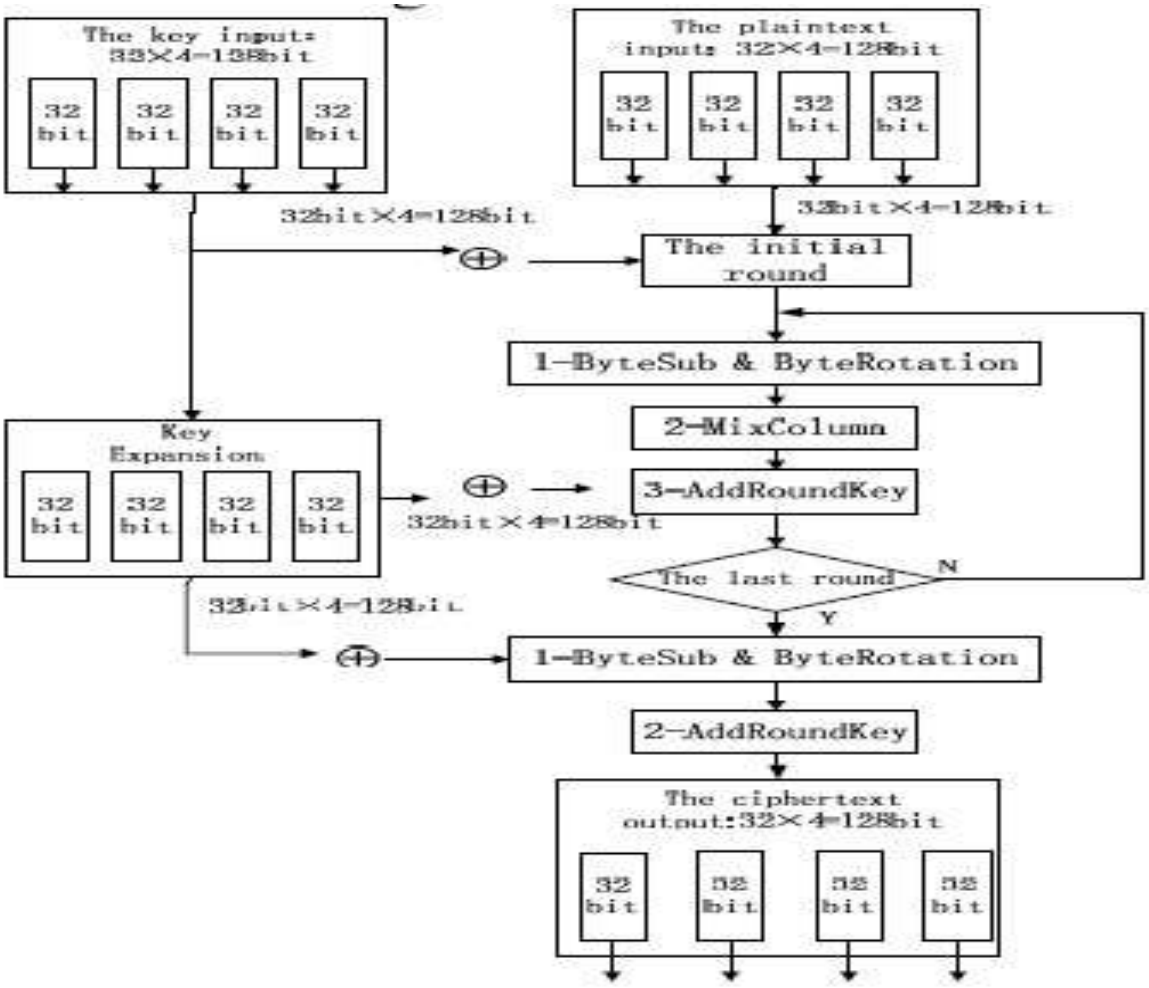


Figure 4. The updated AES algorithm structure

The functions of various parts of the structure shown above are described as follow:

- **The initial round of encryption**:

  One hundred and twenty-eight bits are included in each of the four packets that carry the sequential 32-bit plaintext. At the same time, four consecutive packets of 32-bit initial keys totalling 128 bits have been loaded into other registers. This was done in accordance with the direction of the enable clock signal. Additionally, it is anticipated that this module will make use of the XOR operations combine the plaintext and the fundamental key.

- **Round Transformation in the intermediate steps**:

  The round transformation is the primary method that SubBytes and MixColumns use when dealing with columns that are 32 bits in size. It is necessary to do separate processing on each of the four round transformation packets. XOR operators are then used to combine the 32-bit keys that were obtained through the Keyexpansion process with the result of the MixColumns function. In this particular instance, the round transformation is a 32-output module that accepts 64-input ports containing 32-bit plaintext and 32-bit key entries.

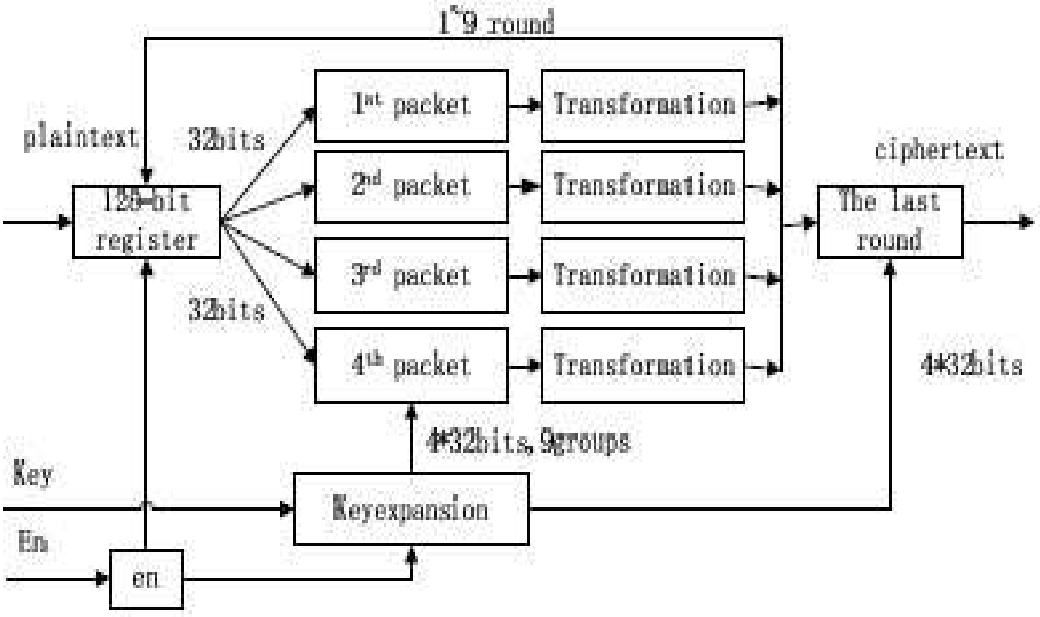


Figure 5. Using pipeline technology for circular processing

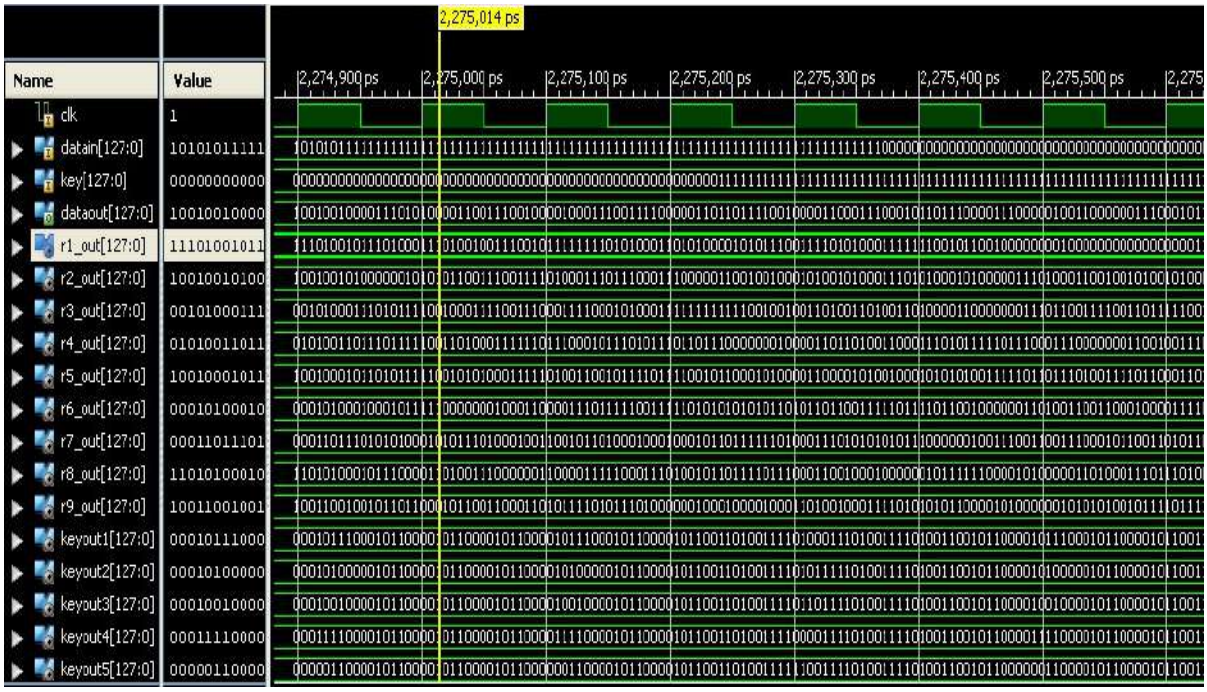
For the purpose of pipelining, four 32-bit packets that each contain 128 bits of data are individually subjected to round transformation.

Through the use of pipelining technology, it is possible to process the four data sets that were previously discussed. To provide a brief summary, it may be described as follows: The raw data should be stored in the 128-bit register

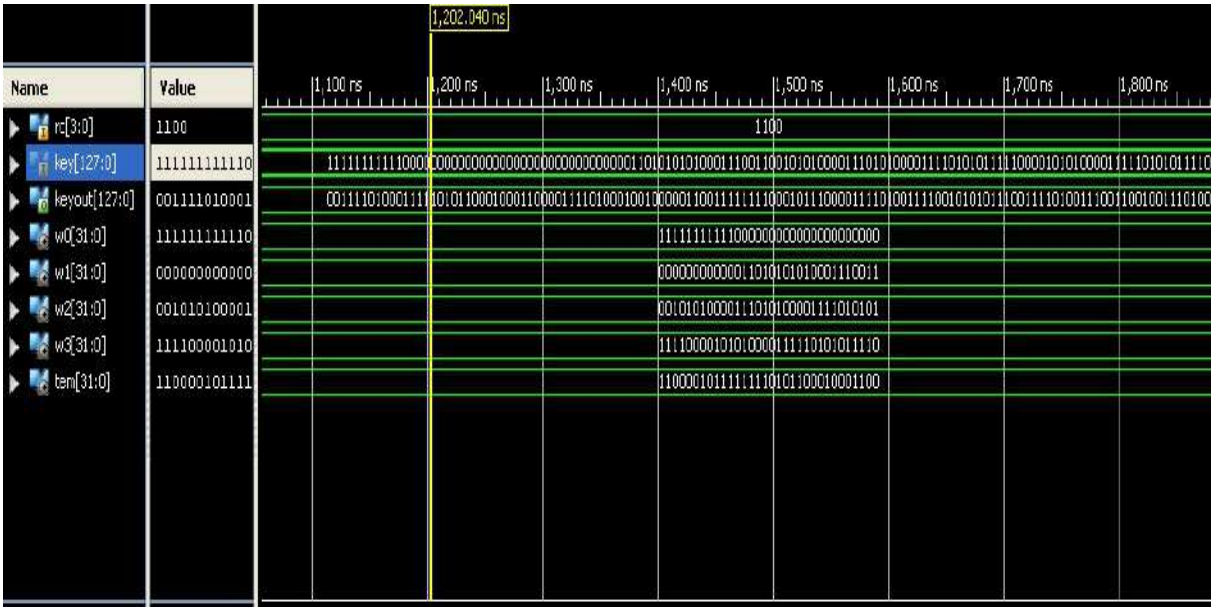
until the operations for the four groups have been completed. After that, the clock should be set to restart the register so that it may read the modified data. The outcome of this is that the 128-bit ROA has been divided into four ROA components that are 32 bits each. get the ciphertext with a length of 128 bits, it is necessary to implement the internal pipelining operation across all nine intermediate Round Transformations of the four packets.

IV. RESULTS

A. SIMULATION FOR AES:



B. SIMULATION FOR KEY EXPANSION:



C. SIMULATION FOR AES_SBOX:

V. CONCLUSION AND FUTURE SCOPE

The purpose of this study is to provide an FPGA implementation of an area-optimized AES algorithm that is acceptable for use in the real world.After being developed in Verilog Hardware Description Language, the waveform of the new algorithm was simulated using many different software programs, including ModelSim SE PLUS 6.0 and Quartus 7.2. At this point, the synthesis simulation of the new approach has been effectively finished.

achieve effective optimisation of the chip space, the design makes use of pipelining technology and a particular data transfer mechanism. This is shown by the results. Because power consumption is related to chip area, this arrangement also minimises the amount of power that is used, which is a very positive aspect. Accordingly, the encryption method that is used in this manner could be able to accomplish certain useful applications.

With this design, it is still feasible to optimise the chip area and power consumption. This is because the S-box is implemented using a look-up table, which allows for easier optimisation. For this reason, the manner in which S-box is implemented need to be the primary focus of research in the future. The application of mathematics in the Galois field (28) to the implementation of the AES algorithm's bytes substitution is yet another promising route for further research in the present and future.

REFERENCES:

[1] J.Yang, J.Ding, N.Li and Y.X.Guo,"FPGA-based design and implementation of reduced AES algorithm" IEEE Inter.Conf. Chal Envir Sci Com Engin(CESCE).,Vol.02, Issue.5-6, pp.67-70, Jun 2010.

[2] A.M.Deshpande, M.S.Deshpande and D.N.Kayatanavar,"FPGA Implementation of AES Encryption and Decryption"IEEE Inter.Conf.Cont,Auto,Com,and Ener., vol.01,issue04, pp.1-6,Jun.2009.

[3] Hiremath.S. and Suma.M.S.,"Advanced Encryption Standard Implemented on FPGA" IEEE Inter.Conf. Comp Elec Engin.(IECEE),vol.02,issue.28,pp.656-660,Dec.2009.

[4] Abdel-hafeez.S.,Sawalmeh.A. and Bataineh.S.,"High Performance AES Design using Pipelining Structure over GF(28)" IEEE Inter Conf.Signal Proc and Com.,vol.24-27, pp.716-719,Nov. 2007.

[5] Rizk.M.R.M. and Morsy, M., "Optimized Area and Optimized Speed Hardware Implementations of AES on FPGA", IEEE Inter Conf. Desig Tes Wor.,vol.1,issue.16,pp.207-217, Dec. 2007.

[6] Liberatori.M.,Otero.F.,Bonadero.J.C. and Castineira.J. "AES-128 Cipher.High Speed, Low Cost FPGA Implementation", IEEE Conf. Southern Programmable Logic(SPL), vol.04, issue.07, pp.195-198, Jun. 2007.

[7] Abdelhalim.M.B., Aslan.H.K. and Farouk.H. "A design for an FPGA based implementation of Rijndael cipher",ITICT. Ena TechSoc.(ETNKS), vol.5,issue.6, pp.897-912, Dec.2005.