IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 09, 2021

OPTIMIZED AREA AND SPEED ARCHITECTURES FOR THE MIX COLUMN OPERATION OF THE ADVANCED ENCRYPTION STANDARD

[1]Aade Kailas Ukala,[2]Lingampally Shivprasad,[3]U.Alekya,[4]Mr. Preethi

[1234]Assistant Professor

Department Of ECE

Kshatriya College of Engineering

ABSTRACT

This project plays vital role in all type of communication applications. This project designs a novel low-transition linear feedback shift register (LFSR) that is based on some new observations about the output sequence of a conventional LFSR. Security of a hardware implementation can be compromised by a random fault or a deliberate attack. The traditional testing methods are good at detecting random faults, but they do not provide to secure all type of attacks. It requires a small set of deterministic tests to cover maximum percentage of single stuck-at faults. Thus, the test execution time is much shorter (at least two orders of magnitude). It has a higher resistance against stuck-at fault type of hardware Trojans. Further, this project can be extended to decrease time by using scan bit swapping LFSR. In this algorithm, all test patterns to circuit are generated using low power LFSR and, generated patterns are reordered, in such a way; power will be decreased while testing application. Latecny reduction can be done by using scan chain reordering. Cell reordering plays vital role in transitions reduction to further improvement of timing constraint.

1. INTRODUCTION

THE fast development of Internet-of-Thing (IoT) devices enables the massive integration of technologies from sensing technology, communication technology, data processing, to cloud computing, and artificial intelligence. In this scenario, sensors in the perception layer collect data from the environment and do fast processing. Then, these data are transmitted through the network layers over the Internet to the cloud. In the cloud, data are further processed by different applications, for example, big data applications or data miningapplications to make decisions and/or to notify users, etc. However, IoT devices and data transmitted through multilayer networks may contain private data or secrete data; while the Internet environment exposes security issues such as personal privacy, cyber-attacks, and organized crimes. This recently raises the concerns about the security and privacy of the IoTs . The solution to security and privacy problems is to include security features such as device identification, device/user authentication, and data encryption. These security functions are often based on the cryptographic algorithms, including public-key cryptography and symmetric cryptography, which occupy processing power and increase power and energy consumption. In contrast, IoT devices are supposed to be constrained low-cost devices with limited processing power, limited memory footprint, and even limited power/energy budget, for example, power-harvesting devices and batterybased devices. This leads to the importance of optimizing cryptographic algorithms in hardware for cost, throughput, and especially power and energy consumption. However, cost, throughput, and power/energy consumption are different features which are hard to achieve at the same time. In this paper, we chose to find a good tradeoff among them for advanced encryption standard (AES) , a widely-

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 09, 2021

used block cipher for emerging IoT proposals, such as IEEE 802.15.4, LoraWAN , Sigfox , and ZWave . We also made comparison with an extreme lightweight data encryption algorithm PRESENT , a candidate for highly constrained devices. PRESENT is a hardware-oriented block cipher with reduced security level but it has small area footprint and very lowpower consumption. However, to the best of our knowledge, lightweight block ciphers, such as PRESENT, are not yet adopted to any IoT proposals. From its standardization in 2001 by the U.S. National Institute of Standards and Technology (NIST) to replace data encryption standard, AES has been studied by researchers in terms of security, performance, and hardware/software implementations. In terms of security, different IoT applications may require different security levels with different power/energy budgets and different throughputs. At the algorithmic level, security level depends on the design of the algorithm and the length of the key. AES supports multiple security levels by providing three different key sizes. AES is proven to support long-term and very long-term security. Because of its popularity and proved security, AES is widely used in data encryption, security protocols, and secure applications. The optimization for AES in hardware is not only beneficial to IoT applications but also to other applications, which have the same constraints. In terms of implementation and performance, AES is designed to benefit from software optimization in modern computing systems. However, AES implementation in software not only introduces delay to data processing and transmission, but also increases the power and energy consumption. This is the main limitation of AES to constrained devices. This leads to the needs of hardware implementation of AES for constrained devices and very high-performance applications. For high-performance applications, hardware AES is often designed using full-parallel architectures , unroll architectures , or pipeline architectures. These architectures can provide high performances, but they have a high occupied area and large-power consumption. In contrast, the AES implementations that are optimized for constrained devices often use serial architectures such as 8-b architectures withone or two S-boxes to save implementation area and to reduce power consumption. The disadvantage of these architectures is the low throughput because of serialization. To optimize for power and/or energy consumption, the architecture for constrained devices can be used with the technology optimizations such as subthreshold voltage and back-biasing.Now a day's most of the users are rapidly using wireless communication technology, and in this wireless communication they are both advantages and disadvantages. We will overcome some disadvantage in wireless communication like hacking process with our project to protect the information from the hacker we are having three types of techniques and are listed below in this chapter:

1. AES (Advanced Encryption Standards)
2. DES (Data Encryption Standards)
3. SEA (Scalable Encryption Algorithm)

These three techniques are certified by National Institute of Standards Techniques (NIST) publications, Information Technology Management, Computer Security.

1.1 EXISTING SYSTEM:-

In previous techniques like DES and SEA have some disadvantages that are when the key and algorithm is known the information can easily hack by unauthorized persons and another disadvantage is high complexity and low security.

DES (DATA ENCRYPTION STANDARDS):-

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 09, 2021

Technology after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106), and the Computer Security Act of 1987 (Public Law 100-235).

The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security to its electronic data systems. This publication specifies two cryptographic algorithms, the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA) which may be used by Federal organizations to protect sensitive data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. The Data Encryption Standard is being made available for use by Federal agencies within the context of a total security program consisting of physical security procedures, good information management practices, and computer system/network access controls. This revision supersedes FIPS 46-2 in its entirety.

EXPLANATION:

The Data Encryption Standard (DES) specifies two FIPS approved cryptographic algorithms as required by FIPS 140-1. When used in conjunction with American National Standards Institute (ANSI) X9.52 standard, this publication provides a complete description of the mathematical algorithms for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithms described in this standard specify both enciphering and deciphering operations which are based on a binary number called a key.

A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key Odd, i.e., there is an odd number of "1"s in each 8-bit byte1. A TDEA key consists of three DES keys, which are also referred to as a key bundle. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. The encryption algorithms specified in this standard are commonly known among those using the standard. The cryptographic sometimes keys are generated in an encrypted form. A random 64-bit number is generated and defined to be the cipher formed by the encryption of a key using a key encrypting key. In this case the parity bits of the encrypted key cannot be set until after the key is decrypted. Security of the data depends on the security provided for the key used to encipher and decipher the data. Data can be recovered from cipher only by using exactly the same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, it may be feasible to determine the key by a brute force “exhaustion attack.” Also, anyone who does have the key and the algorithm can easily decipher the cipher and obtain the original data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.

Data that is considered sensitive by the responsible authority, data that has a high value, or data that represents a high value should be cryptographically protected if it is vulnerable to

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 09, 2021

unauthorized disclosure or undetected modification during transmission or while in storage. A risk analysis should be performed under the direction of a responsible authority to determine potential threats. The costs of providing cryptographic protection using these standard as well as alternative methods of providing this protection and their respective costs should be projected. A responsible authority then should make a decision, based on these analyses, whether or not to use cryptographic protection and this standard.

ADVANTAGES:-

- Security will provided
- It can handle Data up to: 64 bits, Key up to: 56 bits.

DISADVANTAGES:-

- If the key is known hackers can easily hack the data.
- These are the independent variables.

APPLICATIONS:-

- Under Defense system
- Bio medical field

2. PROPOSED SYSTEM:-

ADVANCED ENCRYPTION STANDARD (AES):-

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.

Rijndael was designed to handle additional block sizes and key lengths; however they are not adopted in this standard. Throughout the remainder of this standard, the algorithm specified here in will be referred to as "the AES algorithm." The algorithm may be used with the three different key lengths indicated above, and therefore these different "flavours" may be referred to as "AES-128", "AES-192", and "AES-256".

This specification includes the following sections:

1. Definitions of terms, acronyms, and algorithm parameters, symbols, and functions.
2. Notation and conventions used in the algorithm specification, including the ordering and numbering of bits, bytes, and words.
3. Mathematical properties that is useful in understanding the algorithm.
4. Algorithm specification, covering the key expansion, encryption, and decryption routines.
5. Implementation issues, such as key length support, keying restrictions, and additional block/key/round sizes.

The standard concludes with several appendices that include step-by-step examples for Key. At the start of the Cipher, the input is copied to the State array using the conventions. After an initial Round Key addition, the State array is transformed by implementing a round function 10, 12, or 14 times (depending on the key length), with the final round differing slightly from the first Nr -1 rounds. The final State is then copied to the output.

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 09, 2021

The round function is parameterized using a key schedule that consists of a one-dimensional array of four-byte words derived using the Key Expansion routine.

The Cipher is described in the pseudo code. The individual transformations - Sub Bytes (), Shift Rows (), Mix Columns (), and AddRoundKey () – process the State and are described in the following subsections.

All Nr rounds are identical with the exception of the final round, which does

Not include the Mix Columns () transformation.

DIFFERENCE BETWEEN PROPOSED & EXISITING SYSTEM:-

EXISTING SYSTEM	PROPOSED SYSTEM
1. RCON is fixed. 2. MIXED MULTIPLICATION is also fixed. 3. It can handle Data up to: 64 bits & Key up to: 56 bit. 4. Not much secure, since all blocks are not dependent. 5. KEY is same for all blocks. 6. KEY,USER are dependent 7. It Feistel network	1. RCON is varied. 2. MIXED MULTIPLICATION is also not fixed. 3. It can handle Data up to: 128,192,256 bits & Key up to: 128,192,256. 4. More secure, since all blocks are dependent. 5. KEY is not same for all blocks. 6. KEY,USER are independent 7. Substitution permutation network

Table 2.1: Difference between Proposed & Existing Systems

3. LITERATURE SURVEY

ADVANCED ENCRYPTION STANDARD (AES) IMPLEMENTATION:

On October, 2, 2000, The National Institute of Standards and Technology (NIST) announced Rijndael as the new Advanced Encryption Standard (AES).The Predecessor to the AES was Data Encryption Standard (DES) which was considered to be insecure because of its vulnerability to brute force attacks. DES was a standard from 1977 and stayed until the mid 1990's. However, by the mid 1990s, it was clear that the DES's 56-bit key was no longer big enough to prevent attacks mounted on contemporary computers, which were thousands of times more powerful than those available when the DES was standardized. The AES is a 128 bit Symmetric block Cipher. This thesis includes the complete step by step implementation of Advanced Encryption Technique, i.e. encrypting and decrypting 128 bit data using the AES and it's modification for enhanced reliability and security. The encryption process consists of the combination of various classical techniques such as substitution, rearrangement and transformation encoding techniques. The encryption and decryption modules include the Key Expansion module which generates Key for all iterations. The modifications include the addition of an arithmetic operation and a route transposition cipher in the attacks iterative rounds. The Key

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 09, 2021

expansion module is extended to double the number of iterative processing rounds in order to increase its immunity against unauthorized attacks.

An Advancedand Low Power List For Cryptographic Applications:

The main motive of our project is to design a crypto device with low complexity and high security by using Advanced AES Algorithm using LBIST concept and bit swapping LFSR. The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security to its electronic data systems. There are two main functions that must be performed on-chip in order to implement this: test pattern generation and output response analysis. To accomplish high security for a system we are using the crypto devices technique in our project. Most of the user now a day's using wireless communication for fast sending and receiving the mails in less time and in less cost. When this way of communication is going on, the unauthorized people who have the intension to know about our conversion will hack the information within that frequency. After hacking the information the hacker can know about what we are discussing. This leads to leakage of information to protect that from the hacker we are using Advanced AES algorithm. Further this project is enhanced by increasing the input s of crisp to device. Along with that accessing time of substitution box is decreased by using pipelining concept. Scan chain reordering with all above enhancements decreases power consumption and accessing time of overall project.

Design Of High Secure And Efficient Fsr Based Lbistcryptographic System:

Now a day's most of the users are using wireless communication for fast sending and receiving the mails in less time and in less cost. The main issue in this way of communication is information hacking. Here a crypto device with low complexity and high security is designed by using Advanced Encryption Standard Algorithm along with Built in Self-Test technique. This paper provides the complete step by step implementation of Advanced Encryption Technique, i.e. encrypting and decrypting 128 bit data using the AES by providing enhanced reliability and security. Extra cost in terms of area is very low compared to other techniques. Because only one AES core will be originally embedded in the system. This reduces the reduction of test cost will lead to the reduction of overall production cost & 100% security of data**.**

4. BLOCK DIAGRAMS

In this chapter we will discuss about the block diagrams involve in our entire project.

4.1 OVER ALL CIRCUIT DIAGRAM:-

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 09, 2021

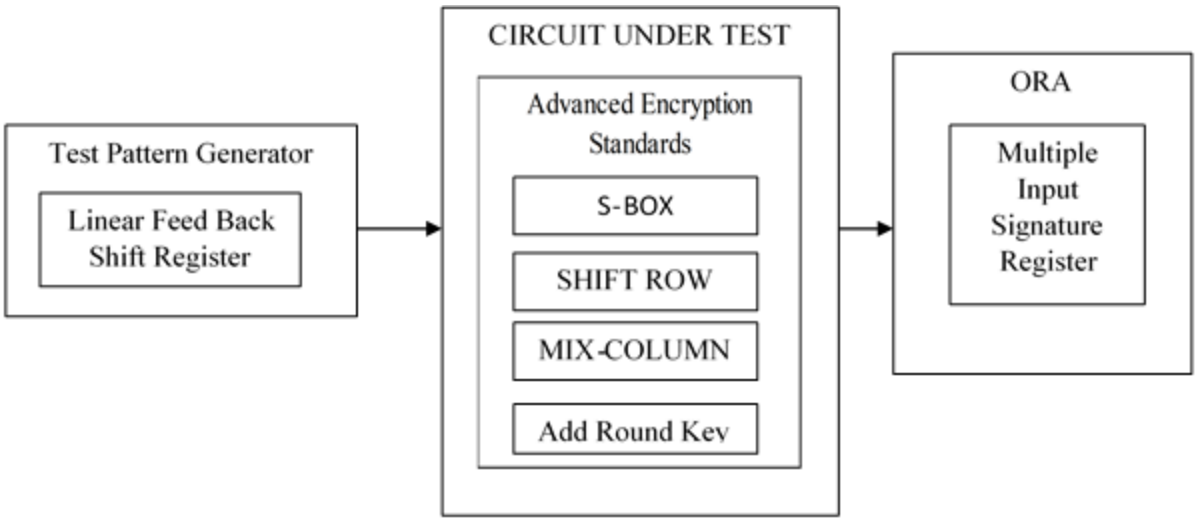


Fig 4.1: Self-Test Technique for Crypto Devices

Above main block diagram shows the overall architecture of LBIST with AES. Starting block linear feedback shift register is used for Test pattern Generator. In computing, a linear-feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. The most commonly used linear function of single bits is exclusive-or (XOR). Thus, an LFSR is most often a shift register whose input bit is driven by the XOR of some bits of the overall shift register value.It is used to generate all type of test patterns for Circuit under Test. Here, in this concept 128 bit LFSR is used as test pattern generator. $2^{128} - 1$ patterns are generated by using above LFSR. Since, XOR gate is used to construct LFSR, all zeros combination is can't be generated.

Here, in above block Circuit Under test is AES block. The Advanced Encryption Standard (AES), also known as Rijndael[4][5] (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is based on the Rijndael cipher[5] developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process.[7] Rijndael is a family of ciphers with different key and block sizes. 128 bit AES is implemented in this project. AES consist 10 rounds as its functionalities. AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware.[10] Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

Output Response Analyzer is last and vital device in this project. Final output checking is done by this component. If any error occurred in whole process or not is checked by this ORA. ORA takes input from AES practical circuit and theoretical circuit, it compares bothinputs using XOR gates, yields final output. 128 xor gates are used to compare produced outputs.

Random pattern testability of crypto-cores has been discussed in this process. Authors show how random data and possible errors can be easily propagated through typical operations involved in symmetric block encryption algorithms. The project focus on data paths of

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 09, 2021

nonstandard algorithms (e.g., 3-WAY cipher) and the test solution lies on a classical centralized BIST architecture where extra test resources are inserted in the design for test pattern generation (TPG) and output response analysis (ORA) functions. Authors in proposed a self-test procedure for a 128-bit key AES core. The inner cyclic behavior is exploited to test the hardware of the round while the key generation module is tested using patterns from the round output. Faults on the control part are not considered. Authors claim 0.76% of area overhead for self-test mode implementation and a testlength of 12 ciphering cycles. In this project, we propose a BIST solution for crypto-devices implementing standard symmetric block cipher algorithms DES and AES. This is an extension of the work presented in that focuses on a specific AES architecture only. Efficient circular self-test schemes as well as TPG and ORA functions are easily implemented on AES and DES crypto-cores due to the iterative process involved in their algorithms. Efficiency of test modes (SELF_TEST, TPG, ORA) in terms of randomness, aliasing, and cost of implementation are discussed and supported by above block diagram.

BLOCK DIAGRAM FOR ENCRYPTION &DECRYPTION:-Plain text key

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 09, 2021

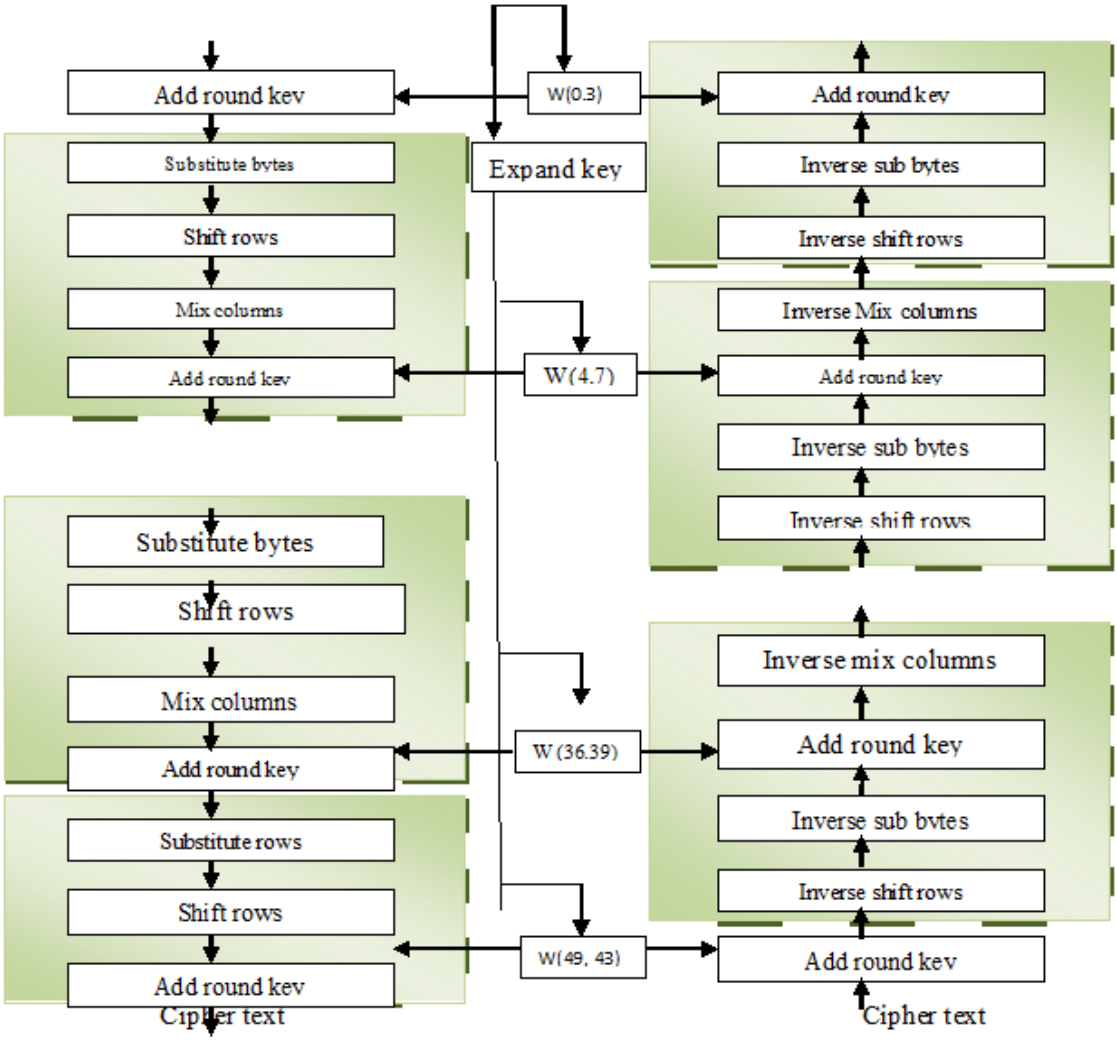
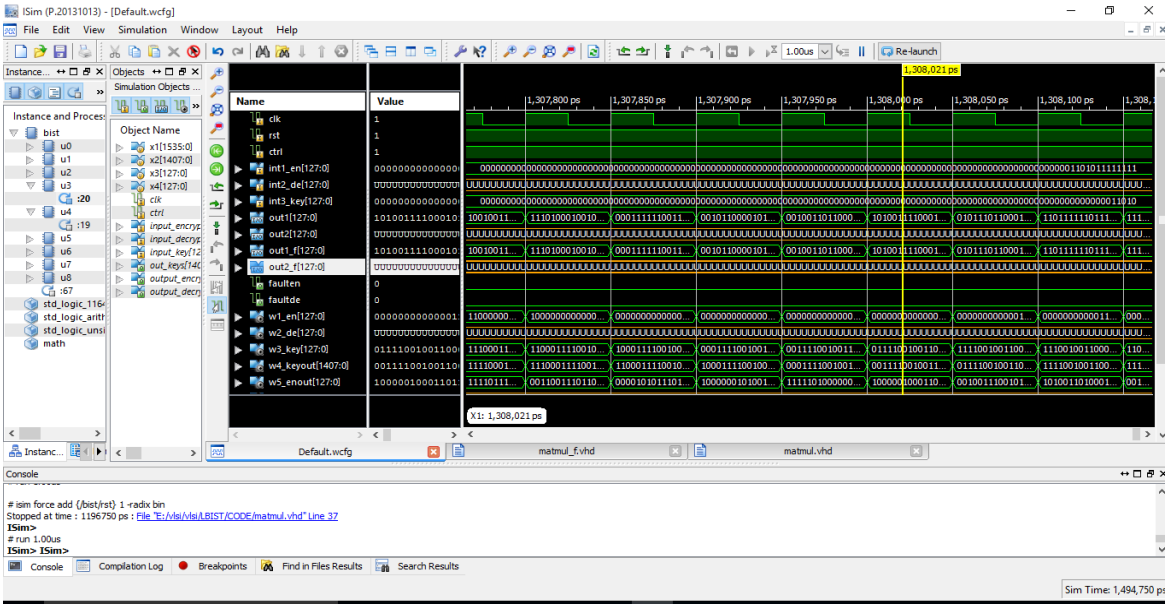


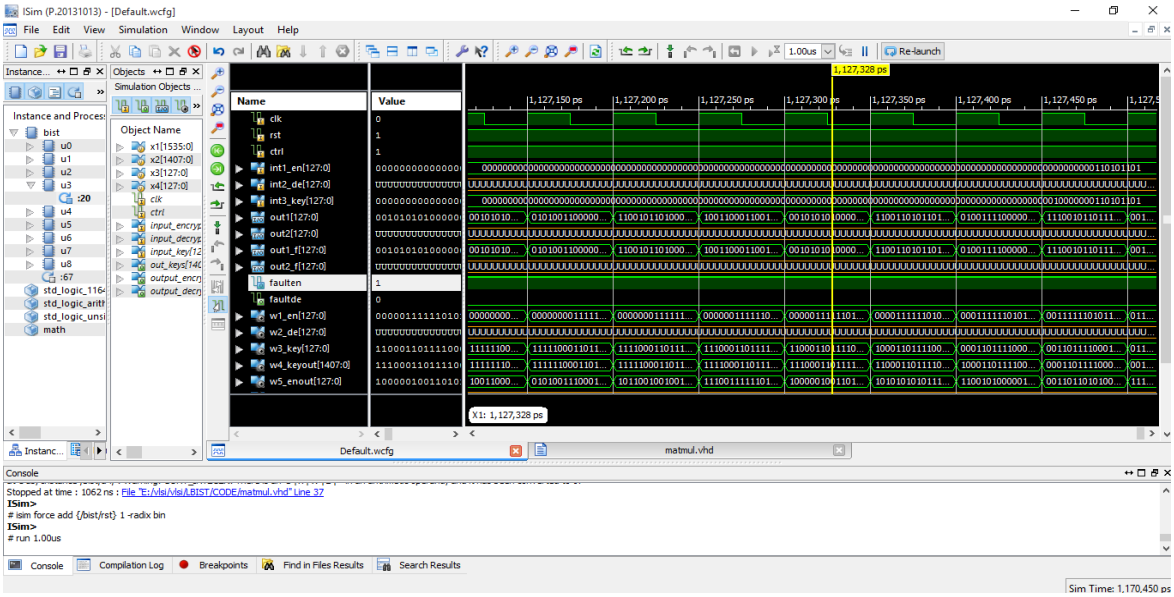
Fig 4.2: Encryption & Decryption block diagram

5. RESULT:

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 09, 2021





EXISTING TIME:

Timing Summary:

Minimum period: 2.584ns (Maximum Frequency: 387.019MHz)

Minimum input arrival time before clock: 4.642ns

Maximum output required time after clock: 4.796ns

Maximum combinational path delay: No path found

PROPOSED TIMING

Timing Summary:

Minimum period: 2.552ns (Maximum Frequency: 391.788MHz)

Minimum input arrival time before clock: 4.642ns

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 09, 2021

Maximum output required time after clock: 4.764ns

Maximum combinational path delay: No path found

6. CONCLUSION:

Crypto may be seen as a continuous struggle between cryptographers & cryptanalysts. Attacks on cryptography have an equally long history. The security of cryptographic modules for providing a practical degree of protection against white-box (total access) attacks should be examined in a totally un-trusted execution environment.

So many developers design so many devices to protect the data very powerful when it is done right, but it is not a panacea. But by using this crypto devices technique we are providing secure scan architecture can easily be integrated into the scan-based DFT design flow as the synthesis register can be specified to the corresponding bit of the secret key. The secure control circuit & multiplexers between the MKR & secret key can be inserted.

In this project a solution is presented that consists in using an AES-based cryptographic core commonly embedded in secure system. Three addition modes are added to the current mission of the AES crypto core. One for pseudo-random test pattern generation & one for signature analysis. Efficiency of these three modes has been demonstrated. Extra cost in terms of area is very low compared to other techniques. Because only one AES core will be originally embedded in the system. This reduces the reduction of test cost will lead to the reduction of overall production cost & 100% security of data.

FUTURE ENHANCEMENT:-

In this project we are designing a crypto devices with low complexity and high security which having the data and key length of 128.futher we can extend the keyand data upon to 192 and 256 bits efficiently and successfullyby using the same technique.

7. REFERENCES

1. S. Reddy, “Easily testable realizations for logic functions,” IEEE Transactions on Computers, vol. 21, no. 11, pp. 1183–1188, 1972.
2. S. Golomb, Shift Register Sequences. Aegean Park Press, 1982.
3. R. K. Brayton, C. McMullen, G. Hatchel, and A. Sangiovanni-Vincentelli, Logic Minimization Algorithms For VLSI Synthesis. Kluwer Academic Publishers, 1984.
4. E. McCluskey, “Built-in self-test techniques,” IEEE Design and Test of Computers, v Vol. 2, pp. 21–28, 1985.
5. D. H. Green, “Families of Reed-Muller canonical forms,” International Journal of Electronics, vol. 70, pp. 259–280, 1991.
6. M. Abramovici, M. A. Breuer, and A. D. Friedman, Digital Systems Testing and Testable Design. Jon Willey and Sons, New Jersey, 1994
7. H.-J. Wunderlich, “BIST for systems-on-a-chip,” Integration, the VLSI Journal, vol. 26, no. 1-2, pp. 55 – 78, 1998.
8. M.G. Kuhn, R.J. Anderson. Soft tempest: hidden data transmission using electromagnetic emanations. Information Hiding 1998,LNCS 1525,pp.124-142,1998.
9. D. Bleichenbacher. Chosen Cipher text Attacks against Protocols Based on the RSA Encryption Standard PKCS #1. CRYPTO'98, LNCS 1462, pp.1-12, 1998.
10. K.Gandolfi,C.Mourte,F. Olivier. Electromagnetic Analysis: Concrete

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 09, 2021

Results. CHES 2001,LNCS 2162,pp.251-261, 2001.

11. J.J. Quisquater, D. Samyde. Electromagnetic analysis (EMA): measures and counter measures for smart cards. E-smart 2001,LNCS 2140,pp.200–210,2001.
12. D.Agrawal, B.Archambeault, J.R.Rao, P.Rohatgi. The EM Side–Channel(s). CHES 2002,LNCS 2523,pp.29-45,2003.
13. Y. Ishai,A. Sahai,D. Wagner. Private Circuits: Securing Hardware against Probing Attacks. CRYPTO 2003, LNCS 2729, pp.463-481, 2003.