ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Efficient VLSI Design of AES Cryptography Based on DNA Design

G. Siva Ramakrishna
Department of Electronics & Communication Engineering,
Kakinada Institute of Technology and Science,
Divili, Samalkot, Andhra Pradesh 533433, India.

B.Raja Rao
Department of Electronics & Communication Engineering,
Kakinada Institute of Technology and Science,
Divili, Samalkot, Andhra Pradesh 533433, India.

ABSTRACT

This paper describes a novel Sub bytes approach for implementation of the advanced encryption standard (AES) algorithm, which provides a significantly improved strength of Cryptography. Our method is based on randomization in composite field arithmetic, which entails a low implementation cost while does not alter the algorithm, does not reduce the working frequency, and keeps perfect compatibility with the published standard. The DNA Encoder, suitable to be integrated in AES Cryptographer, is presented. The DNA Technique is to improve the Security of AES Design. This Proposed AES System with DNA TRNG Implemented using Verilog HDL and Simulated by Modelsim 6.4 c and Synthesized by Xilinx tool. The proposed system implemented in FPGA Vertex or Spartan 3. The proposed AES System has been made into an IP and successfully applied in encryption application.

INTRODUCTION

Cryptography [1], often called encryption, is the practice of creating and using a cryptosystem or cipher to prevent all but the intended recipient(s) from reading or using the information or application encrypted. A cryptosystem is a technique used to encode a message. The recipient can view the encrypted message only by decoding it with the correct algorithm and keys.

Cryptography is used primarily for communicating sensitive material across computer networks. The process [2] of encryption takes a clear-text document and applies a key and a mathematical algorithm to it, converting it into crypto-text [6]. In crypto-text, the document is unreadable unless the reader possesses the key that can undo the encryption. In 1997 the National Institute of Standards and TECHNOLOGY (NIST) [3], a branch of the US government, started a process to identify a replacement for the Data Encryption Standard (DES) [5]. It was generally recognized that DES was not secure because of advances in computer processing power. The goal of NIST was to define a replacement for DES that could be used for non-military information security applications by US government agencies. Of course, it was recognized that commercial and other non-government users would benefit from the work of NIST and that the work would be generally adopted as a commercial standard. The NIST invited cryptography and data security specialists from around the world to participate in the discussion and selection process. Five encryption algorithms were adopted for study. Through a process of consensus the encryption algorithm proposed by the Belgium cryptographers Joan Daeman and Vincent Rijmen was selected. Prior to selection Daeman and Rijnmen used the name Rijndael (derived from their names) for the algorithm. After adoption the encryption algorithm was given the name Advanced Encryption Standard (AES) [7] which is in common use today. In 2000 the NIST formally adopted the AES encryption algorithm and published it as a federal standard under the designation FIPS-197. The full FIPS-197 standard is available on the NIST web site (see the Resources section below).

Cite this article as: G. Siva Ramakrishna & B.Raja Rao, "An Efficient VLSI Design of AES Cryptography Based on DNA Design", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 5 Issue 5, 2018, Page 90-97.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

As expected, many providers of encryption software and hardware have incorporated AES encryption into their products.

AES encryption uses a single key as a part of the encryption process. The key can be 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes) in length. The term 128-bit encryption refers to the use of a 128-bit encryption key. With AES both the encryption and the decryption are performed using the same key. This is called a symmetric encryption algorithm. Encryption algorithms that use two different keys, a public and a private key, are called asymmetric encryption algorithms [8]. An encryption key is simply a binary string of data used in the encryption process. Because the same encryption key is used to encrypt and decrypt data, it is important to keep the encryption key a secret and to use keys that are hard to guess. Some keys are generated by software used for this specific task. Another method is to derive a key from a pass phrase. Good encryption systems never use a pass phrase alone as an encryption key.

EXISTING SYSTEM:

This paper presents novel high-speed architectures for the hardware implementation of the Advanced Encryption Standard (AES) algorithm. Unlike previous works which rely on look-up tables to implement the Sub Bytes and Inv Sub Bytes transformations of the AES algorithm, the proposed design employs combinational logic only. As a direct consequence, the unbreakable delay incurred by look-up tables in the conventional approaches is eliminated, and the advantage of sub pipelining can be further explored [9]. Furthermore, composite field arithmetic is employed to reduce the area requirements, and here Key expansion method was implemented for Random Key Generation. In this method, area and delay was Increased due to Round Key Expansion Process.

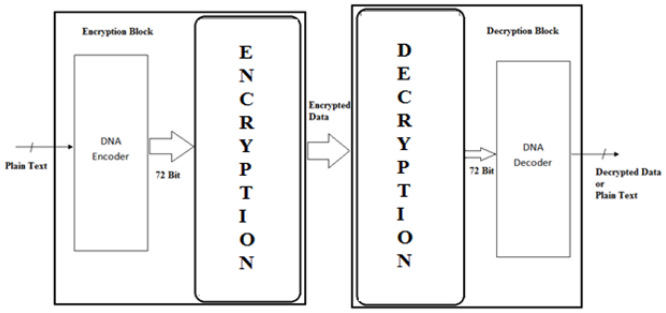
DISADVANTAGE:

- Area is more
- Complex Key Generation Process
- Manual Key Process

PROPOSED SYSTEM:

The proposed method is based on DNA Encoding [10] in the underlying Galois Field of the AES and unlike other countermeasure does not add any additional operation to the algorithm execution flow, does not decrease the working frequency, does not alter the algorithm and keeps perfect compatibility with the published standard. In addition, it does not require pre-computed tables for storing masked values in ROM. This is specifically important for constrained security tokens such as smart cards. We focused on the optimization strategies for 128-b data path architecture to achieve High Security, High-throughput hardware AES encryption module providing multiple levels of security with small area footprint. The area is saved by reorganizing the encryption data path to minimize the number of data registers and combinational logics.

PROPOSED SYSTEM BLOCK DIAGRAM:



PROPOSED SYSTEM TECHNIQUE:

- AES with S-Box Design with DNA Encoder

PROPOSED SYSTEM ADVANTAGES:

- Low Complexity
- Low Power
- Feasible to use for different performance
- Implementation objectives of sensitive smart applications

NOVEL APPROACH TO PROTECT AES ALGORITHM IMPLEMENTATION

Cryptographic architectures provide protection for sensitive and smart infrastructures such as secure healthcare, smart grid, fabric, and home. Cryptography

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

is closely related to the disciplines of cryptology and cryptanalysis [11]. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption) [12]. Individuals who practice this field are known as cryptographers. Nonetheless, the use of cryptographic architectures does not guarantee immunity against faults occurring in these infrastructures. Defects in VLSI systems [13] may cause smart usage models to malfunction. Extensive research has been done for detecting such faults in the cryptographic algorithms such as elliptic curve cryptography and the Advanced Encryption Standard. Design for reliability and fault immunity ensures that with the presence of faults, reliability is provided for the aforementioned sensitive cryptographic architectures.

MODULES SEPERATION:

- Substitution Box (S- Box)
- Multiplier in GF(24)
- Multiplier in GF(22)
- Squarer in GF(24)
- Constant multiplier (×λ)
- Multiplier (×ϕ)
- Addition in GF (24)
- Shift Rows
- Mix Columns
- Add Round Key
- Transformation matrix & inverse transformation matrix
- Key Expansion Unit
- DNA Coder

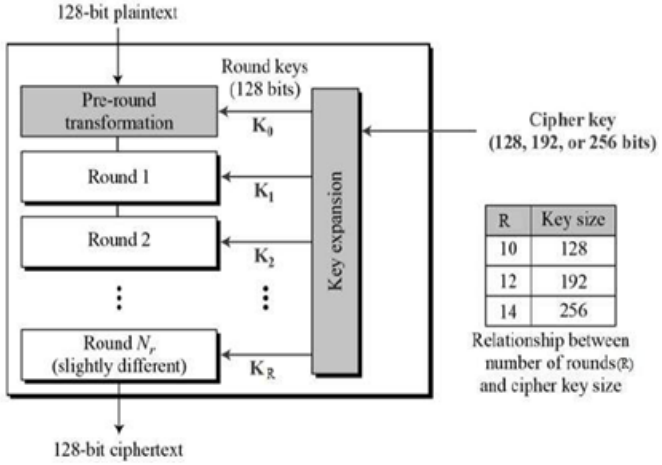
AES ALGORITHM

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES [14] in a number of ways. The algorithm Rijindael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively. As well as these differences AES differs from DES in that it is not a feistel structure. Recall that in a feistel structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. In this case the entire data block is processed in parallel during each round using substitutions and permutations [15].

AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration



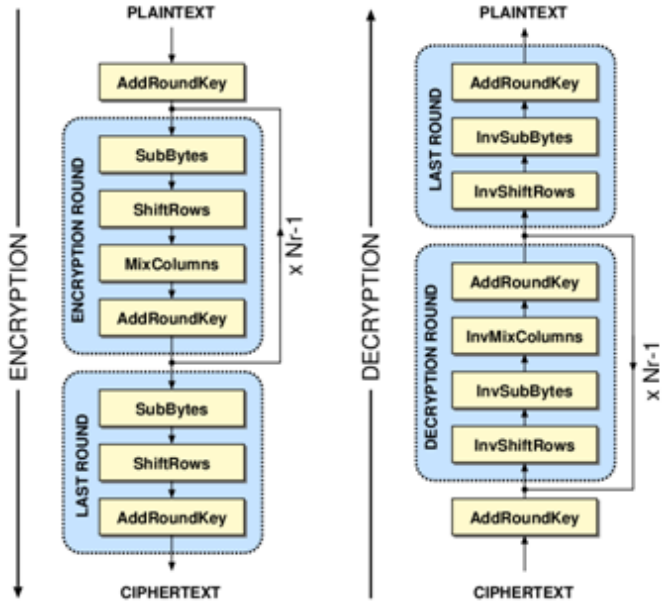
R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The AES Encryption and Decryption process is mentioned in bellow Diagram. The process of decryption of an AES cipher text is similar to the encryption process in the reverse order. Each round consists of the four processes

- Add round key
- Mix columns
- Shift rows
- Byte substitution



APPLICATIONS:

- Data encryption and decryption
- Security system
- Digital information security
- Computer/network security

VLSI:

VLSI stands for "Very Large Scale Integrated Circuits". It's a classification of ICs. An IC of common VLSI includes about millions active devices. Typical functions of VLSI include Memories, computers, and signal processors, etc. A semiconductor process technology is a method by which working circuits can be manufactured from designed specifications. There are many such technologies, each of which creates a different environment or style of design. In integrated circuit design, the specification consists of polygons of conducting and semiconducting material that will be layered on top of each other to produce a working chip. When a chip is custom-designed for a specific use, it is called an application-specific integrated circuit (ASIC). Printed-circuit (PC) design also results in precise positions of conducting materials, as they will appear on a circuit board; in addition, PC design aggregates the bulk of the electronic activity into standard IC packages, the position and interconnection of which are essential to the final circuit. Printed circuitry may be easier to debug than integrated circuitry is, but it is slower, less compact, more expensive, and unable to take advantage of specialized silicon layout structures that make VLSI systems so attractive. The design of these electronic circuits can be achieved at many different refinement levels from the most detailed layout to the most abstract architectures. Given the complexity that is demanded at all levels, computers are increasingly used to aid this design at each step. It is no longer reasonable to use manual design techniques, in which each layer is hand etched or composed by laying tape on film. Thus the term computer-aided design or CAD is a most accurate description of this modern way and seems more broad in its scope than the recently popular term computer-aided engineering (CAE)

APPLICATIONS OF VLSI

Electronic systems now perform a wide variety of tasks in daily life. Electronic systems in some cases have replaced mechanisms that operated mechanically, hydraulically, or by other means; electronics are usually smaller, more flexible, and easier to service. In other cases electronic systems have created totally new applications. Electronic systems perform a variety of tasks, some of them visible, some more hidden:

- Personal entertainment systems such as portable MP3 players and DVD players perform sophisticated algorithms with remarkably little energy.
- Electronic systems in cars operate stereo systems and displays; they also control fuel injection systems, adjust suspensions to varying

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

terrain, and perform the control functions required for anti-lock braking (ABS) systems.

- Digital electronics compress and decompress video, even at high definition data rates, on-the-fly in consumer electronics.
- Low-cost terminals for Web browsing still require sophisticated electronics, despite their dedicated function.
- Personal computers and workstations provide word-processing, financial analysis, and games. Computers include both central processing units (CPUs) and special-purpose hardware for disk access, faster screen display, etc.

SIMULATION IMPLEMENTATION

Verilog HDL is a Hardware Description Language (HDL). A Hardware Description Language is a language used to describe a digital system, for example, a computer or a component of a computer. One may describe a digital system at several levels. For example, an HDL might describe the layout of the wires, resistors and transistors on an Integrated Circuit (IC) chip, i. e., the switch level. Or, it might describe the logical gates and flip flops in a digital system, i. e., the gate level. An even higher level describes the registers and the transfers of vectors of information between registers. This is called the Register Transfer Level (RTL). Verilog supports all of these levels. However, this handout focuses on only the portions of Verilog which support the RTL level.

VERILOG:

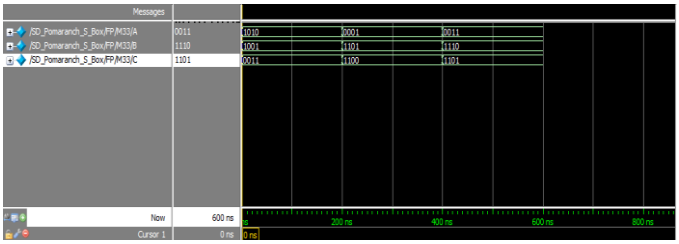
Verilog is one of the two major Hardware Description Languages (HDL) used by hardware designers in industry and academia. VHDL is the other one. The industry is currently split on which is better. Many feel that Verilog is easier to learn and use than VHDL. As one hardware designer puts it, "I hope the competition uses VHDL." VHDL was made an IEEE Standard in 1987 and Verilog in 1995. Verilog is very C-like and liked by electrical and computer engineers as most learn the C language in college. VHDL is very most engineers have no experience. Verilog was introduced in 1985 by Gateway Design System Corporation, now a part of Cadence Design Systems, Inc.'s Systems Division. Until May, 1990, with the formation of Open Verilog International (OVI), Verilog HDL was a proprietary language of Cadence. Cadence was motivated to open the language to the Public Domain with the expectation that the market for Verilog HDL-related software products would grow more rapidly with broader acceptance of the language. Cadence realized that Verilog HDL users wanted other software and service companies to embrace the language and develop Verilog-supported design tools.

SNAPSHOTS

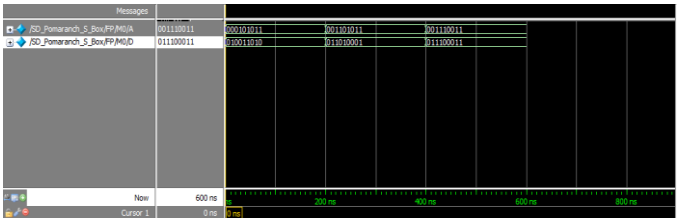
Snapshot is nothing but every moment of the application while running. It gives the clear elaborated of application. It will be useful for the new user to understand for the future steps.

VARIOUS SNAPSHOTS:

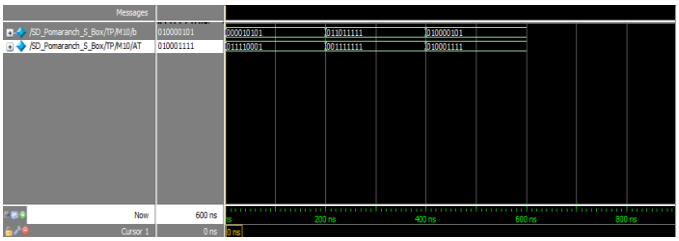
2 BIT ADDER:



DEL Iverse:

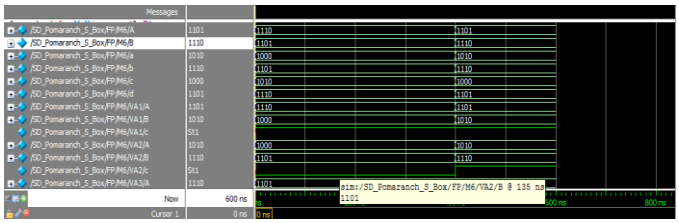


AFFINE TRANSFORM:

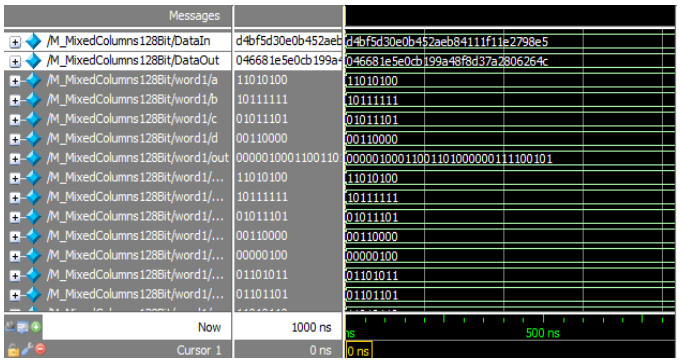


ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

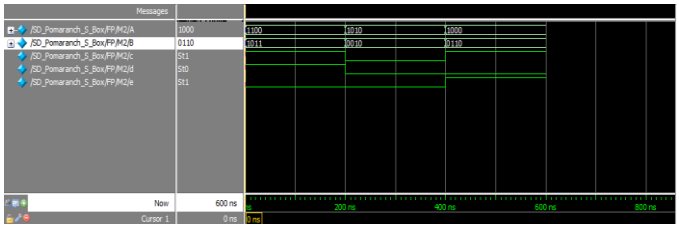
X INVERSE:



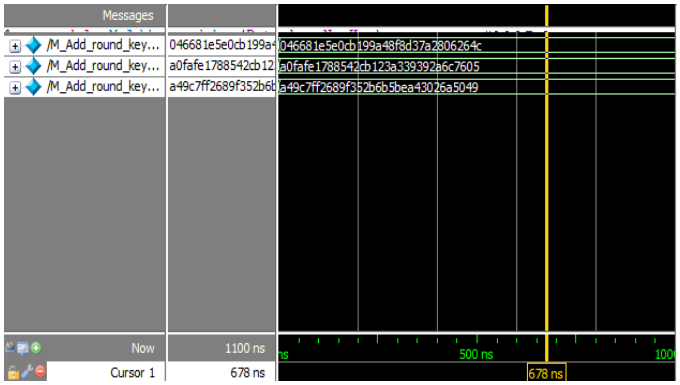
MIXED COLUMN:



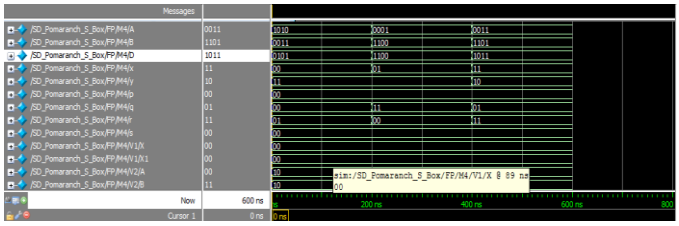
LAMDA:



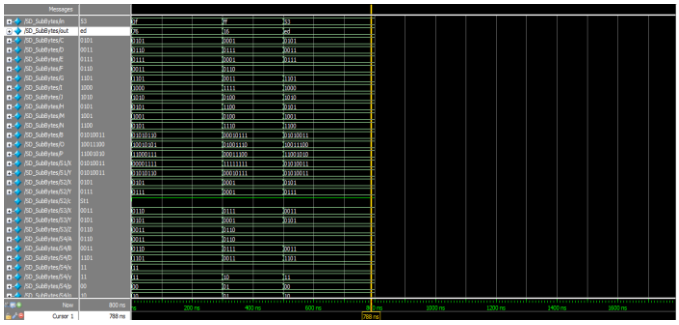
ADD ROUND KEY:



BLACK X BOX:

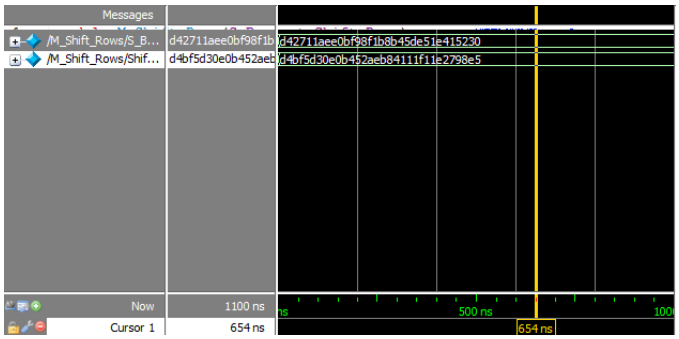


SUB BYTES:

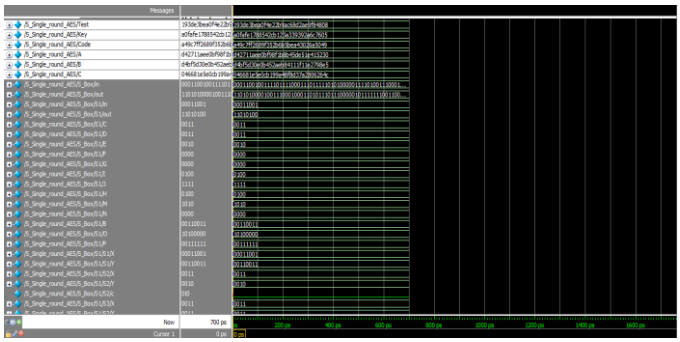


ENCRYPTION:

SHIFT ROWS:

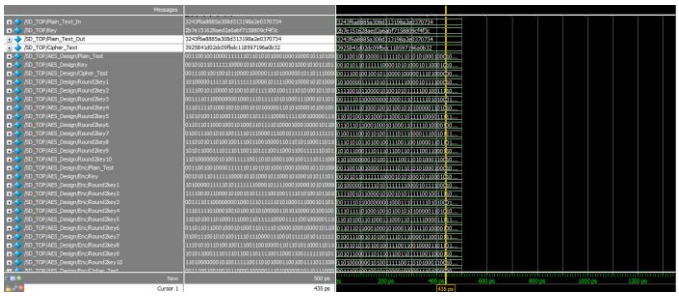


SINGLE ROUND OPERATION:

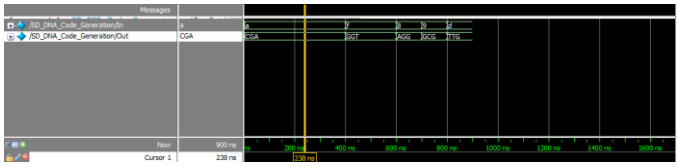


ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

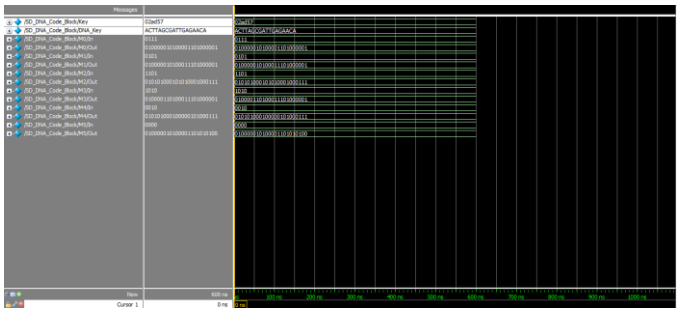
FINAL TOP MODULE:



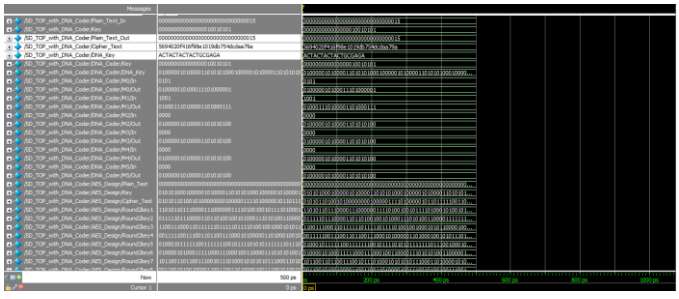
DNA CODE GENERATION:



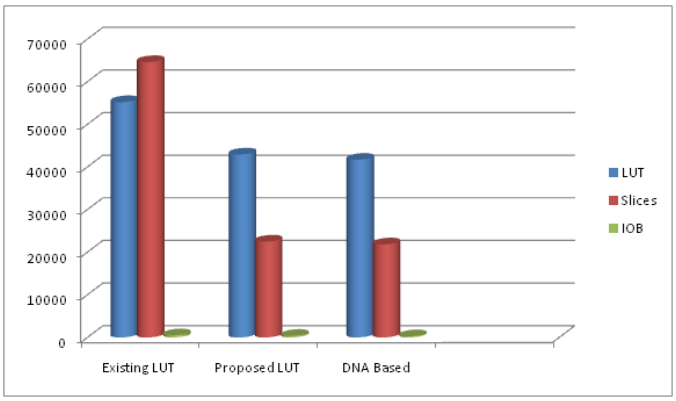
DNA CODE BLOCK:



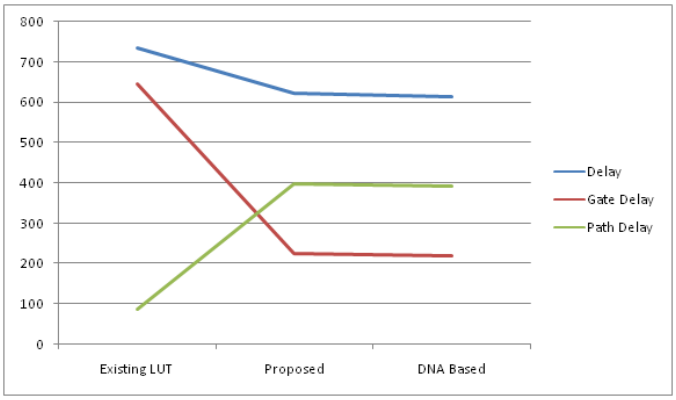
DNA BASED TOP MODULE CRYPTO:



AREA GRAPH:



DELAY GRAPH:



COMPARISON TABLE:

AREA AND DELAY COMMPARISON TABLE

Method Name	Area in Number of LUT			Delay		
Spartan 3 XC 3S 4000L-4FG900	LUT	Slices	IOB	Delay	Gate or Logic Delay	Path or Route Delay
Existing LUT	55226	64627	512	734.2ns	646.5ns logic	87.7ns route
Proposed Design	42933	22510	384	623.168ns	225.498ns	397.671ns
DNA BASED	41697	21844	280	613.140ns	220.653ns	392.487ns

CONCLUSION:

A novel AES Design with DNA implementation with High Security Constrains. The Implementation is based on mathematical properties of Rijndael algorithm and remains based on DNA Coders. Another contribution of this paper is that it designs Encryption Design using Shit rows, Mixed Column, Add Round Key and We Will Design a Decryption Part also. Finally with the help of Genetic Algorithm based Encoding for Key Generation is used for Encryption and Decryption Process. The new design permits the construction of efficient area and speed characteristics, while still keeping a very high protection level. We conducted relevant AES Implementation with DNA for Key Generation Method.

Nearly all the algorithms embedded in Cryptographer have been designed to resist at high level to linear, differential and high order differential attacks, whereas nothing has been done to make them inherently resistant

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

attacks. However, this work will be implemented in the FPGA. It is possible to design algorithms, so when the next generation of cryptographic.

REFERENCES

[1]. K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," Commun. ACM, vol. 56, no. 10, pp. 35–37, Oct. 2013.

[2]. D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," IEEE Pervasive Comput., vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.

[3]. M. Rostami, W. Burleson, A. Jules, and F. Koushanfar, "Balancing security and utility in medical devices?" in Proc. 50th ACM/EDAC/IEEE Int. Conf. Design Autom., May/Jun. 2013, pp. 1–6.

[4]. M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," Proc. IEEE, vol. 102, no. 8, pp. 1174–1188, Aug. 2014.

[5]. H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," IEEE Security Privacy, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.

[6]. M. Mozaffari-Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in Proc. 26th Int. Conf. VLSI Design, Jan. 2013, pp. 203–208.

[7]. R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," Computer, vol. 44, no. 9, pp. 51–58, Sep. 2011.

[8]. T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker, "Challenges in access right assignment for secure home networks," in Proc. USENIX Conf. Hot Topics Secur., 2010, pp. 1–6.

[9]. M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Concurrent structure independent fault detection schemes for the Advanced Encryption Standard," IEEE Trans. Comput., vol. 59, no. 5, pp. 608–622, May 2010.

[10]. M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A low-power high performance concurrent fault detection approach for the composite field S-box and inverse S-box," IEEE Trans. Comput., vol. 60, no. 9, pp. 1327–1340, Sep. 2011.

[11]. M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A lightweight high performance fault detection scheme for the Advanced Encryption Standard using composite fields," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 19, no. 1, pp. 85–91, Jan. 2011.

[12]. A. Satoh, T. Sugawara, N. Homma, and T. Aoki, "High-performance concurrent error detection scheme for AES hardware," in Proc. 10th Int. Workshop CHES, Aug. 2008, pp. 100–112.

[13].P. Maistri and R. Leveugle, "Double-data-rate computation as a countermeasure against fault analysis," IEEE Trans. Comput., vol. 57, no. 11, pp. 1528–1539, Nov. 2008.

[14]. X. Guo and R. Karri, "Recomputing with permuted operands: A concurrent error detection approach," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 32, no. 10, pp. 1595–1608, Oct. 2013.

[15]. M. Mozaffari-Kermani and R. Azarderakhsh, "Efficient fault diagnosis schemes for reliable lightweight cryptographic ISO/IEC standard CLEFIA benchmarked on ASIC and FPGA," IEEE Trans. Ind. Electron., vol. 60, no. 12, pp. 5925–5932, Dec. 2013.