Design and Implementation of Low-power Nanoscale Cryptosystem for Group-centric secure information sharing

Valliyappan Valliyappan*, Eugene B John, Ram Krishnan, and Sruthi Nanduru
The University of Texas at San Antonio, San Antonio, Texas, 78249, USA
kjw322@my.utsa.edu, eugene.john@utsa.edu, ram.krishnan@utsa.edu, kpr934@my.utsa.edu

Abstract

Advancement in technology, creates a dire need of secure data transmission for information exchange. The Data Encryption Standard (DES), Triple Data Encryption Standard (TDES) and Advanced Encryption standard (AES) algorithms are a few of the widely used encryption algorithms for secure data exchange process.In this paper, the integration of different security algorithms via; AES, DES and triple DES in g-SIS on a Single Silicon Die is designed and implemented. The area and power consumption of different algorithms are taken as the evaluation parameters for analysis of the system. The total design is coded using Xilinx ISE and Icarus Verilog, it is synthesized using a cadence RTL compiler and finally the GDS2 layout of the design is implemented using cadence Encounter.

Keywords: Encryption,Decryption,DES,AES,TDES.

1 Introduction

Most of the information in today's world is in digital format. For example photos, music or any other private information which can be transmitted to a recipient anywhere in the world. This gives a great flexibility, but on the other hand, the lack of privacy became an obstacle. However, this obstacle can be overcome by cryptography. Cryptography is devoted to ensure secure transmission of data. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The Data Encryption Standard (DES), known as the Data Encryption Algorithm (DEA) by ANSI and DEA-1 by the ISO, has been a worldwide standard for over 20 years. It's highly influential in the advancement of modern cryptography. But DES is now considered to be insecure for many applications. This is mainly due to 56 bit key size which is considered to be too normalsize. There are some analytical results which demonstrate theoretical weakness in cipher, although they are infeasible to mount in practice. The algorithm is believed to be secure in the form of triple DES, although there are theoretical attacks. Triple DES provides a relatively simple method of increasing the key size of DES, whose main feature is to protect against the DES prone attacks. Another encryption algorithm which supersedes the DES algorithm is AES. Advanced Encryption standard (AES) is also referred as Rijndael which uses a substitution-permutation network, whereas the DES algorithm is based on a Feistel network.

There have been many techniques proposed till date on encryption algorithms. In [7], two cryptographic calculations namely the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA) were presented. In this various steps have been described for conversion of data into

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 1, Article No. 20 (August 31, 2015)
*Corresponding author: Department of Electrical and Computer Engineering, UTSA, 1UTSA Circle, Sanantonio, Texas, 78249, USA, Tel: (210) 458-4011

cryptographic cypher. In [8], an overhead dissection of advanced encryption standard (AES) and its execution in wireless systems was presented. In [4], the limit of the three-node system comprising of a source, an objective, and a relay was described. It can also be observed that when all the nodes were in similar band, the system can be reduced into a broadcast channel from the viewpoint of the source and a different access channel from the point of view of the sink. In [2], a minimal yet fast structural planning for Rijndael was proposed and assessed through the implementation of ASIC. Additionally, the s-box architecture is also optimized. In [9], a novel high-speed architecture based on AES technique was implemented. Also in the proposed configuration, look-up tables were replaced by simple combinational logic and a proficient key extension modeling suitable for the sub-pipelined round units was displayed. In [5], two low-area techniques for AES on FPGAs were displayed. In [1], a comparative analysis between four generally utilized encryption techniques, i.e. DES (Data Encryption Standard), 3DES (Triple DES), BLOWFISH and AES (Rijndael) were made. On investigating the four techniques under diverse programming stage, it has been observed that the Blowfish is the best performing technique based upon security against unapproved attacks.

In this paper, the integration of three different security algorithms viz; AES, DES and triple DES in the Group-Centric Secure Information Sharing model (g-SIS) [6] on a Single Silicon Die is presented. The g-SIS model proposes bringing concerned users and objects (information) in a group for the purpose of access control. The rest of the paper is organized as follows. Section 2 briefly describes the different encryption algorithms. Section 3 discusses the tools and methodology used for implementation. Section 4 gives the simulation results based on the performance of the system. Finally, section 5 presents the conclusion.

2 Algorithm

Encryption is a process of encoding information or data, so that it remains useless to anyone except for the one who possess the appropriate key to decrypt it. Few encryption algorithms are described below.

2.1 DES Algorithm

DES algorithm is designed to encipher and decipher blocks of data consisting of 64 bits along with a 64 bit key (just 56 bits are utilized for conversion reason and the rest of the bits are utilized for parity checking).

For encryption process, initially a plain text of 64bits is subjected to an initial permutation, then to a module where it is computed with the key and finally to the inverse permutation. Then a complex computation of 16 rounds in a Fiestal system network, where each round comprises permutation and substitution of the text bit and the inputted key bit. DES operates in four different modes, namely, ECB (Electronic Codebook mode), CBC (Cipher Block Chaining mode), CFB (Cipher Feedback mode) and OFB (Output Feedback mode). Finally, in the last stage an inverse permutation is made. The security of DES relies upon the fortification of key, which can be done by using Linear Feedback Shift Register or Chaos Logistic Block.The decryption process is the reverse of encryption process. As the key length is normalsize, DES algorithm can experience chosen plain text attacks.

2.2 Triple DES Algorithm

In Triple DES, we apply the DES algorithm three times with a 64 bit plain text with three different keys, which includes 8 rounds of computation. Initially an encryption utilizing DES with the initial 64-bit key is done, then decryption utilizing DES with the second 64-bit key is followed and finally, encryption

utilizing DES with the third 64-bit key is performed. Since Triple-DES applies the DES technique three times, it takes three times the length of standard DES. But TDES is also liable to brute force attacks [3].

2.3 AES Algorithm

AES (Advanced Encryption Standard) was announced by the National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a 5-year institutionalization process. AES has a slight variation from Rijndael in terms of block size and key size. In Rijndael, key size need not match the block size, i.e. the block size can be any multiple of 32 unless it exceeds 128 bits with any key size. Whereas, FIPS-197 specified AES contains 128 bits of block size and its key size may be chosen from a set of 128, 192 and 256 bits.

In general AES uses a substitution permutation network, where each round of processing involves byte-level substitutions followed by word-level permutations. The encryption algorithm of AES includes 9 rounds if the key length is 128 bit, 11 rounds if the key length is 192 bit and 13 rounds if the key length is 256 bit. Each round includes four different stages, one permutation and three substitutions, i.e. bytes substitution transformation, shift rows transformation, mixing of columns transformation and addition of round key transformation. Expect the last round which does not contain mixing of the columns transformation stage. The decryption process is the direct inverse of the encryption process.

In substitute bytes stage, a 16x16 matrix S box is used to perform a byte-by-byte substitution of the block. The shift row transformation operates on the rows of the state, where it cyclically shifts the bytes in each row by a certain offset, leaving the first row unchanged .This has the effect of moving bytes to lower positions in the row, while the lowest bytes wrap around into the top of the row. Mixing of columns transformation operates on each individual column by considering it as a four-term polynomial. This is mainly based on Galois Field multiplication where every byte of a column is supplanted with an alternate value that is a function of each of the four bytes in the given column. The addition of round key transformation is to combine sub-key to the state using basic bitwise xor operation.The application of this transformation to the N_r rounds of the encryption occur when $1 \leq \text{round} \leq N_r$. The key schedule expansion generates a total of $N_b \times (N_r + 1)$ words, where N_r is the number of rounds and each round requiresN_b words of key data. Each round key is a 4-word (128-bit) array generated as a product of the previous round key, a constant that changes every round except the first round key which remains unchanged. Although the AES encryption and decryption ciphers have identical forms of key schedule, they differ in transformation sequencing. Hence, AES beats TDES both in programming and hardware. [8]

3 Tools and Methodology

The AES and DES algorithms are implemented using verilog. Initially, sub-modules are created and called in the top module in a group centric fashion. For low power implementation, all the modules were clock gated and power gated. Also DVFS (Dynamic Voltage and Frequency scaling) technique has been considered for more aggressive power reduction. User authentication module or top module defines the behavior of an individual to access the desired object as shown in figure1.

The 128 bit data was encrypted for the generation of cipher text. As TDES is a 64 bit algorithm, it is implemented in two parallel modes i.e. from 0:63 and 64:127 bits, in order to compensate the input requirement. Instead of comparing two architectures, the results of each algorithm are obtained in a serial manner. AES and TDES algorithms are compared by enabling a top module with a pin that toggles among the two algorithms. That is a selection line (which is not specified in figure 1) is used to choose the encryption method that can prevent the un-necessary computational expanse that could have been

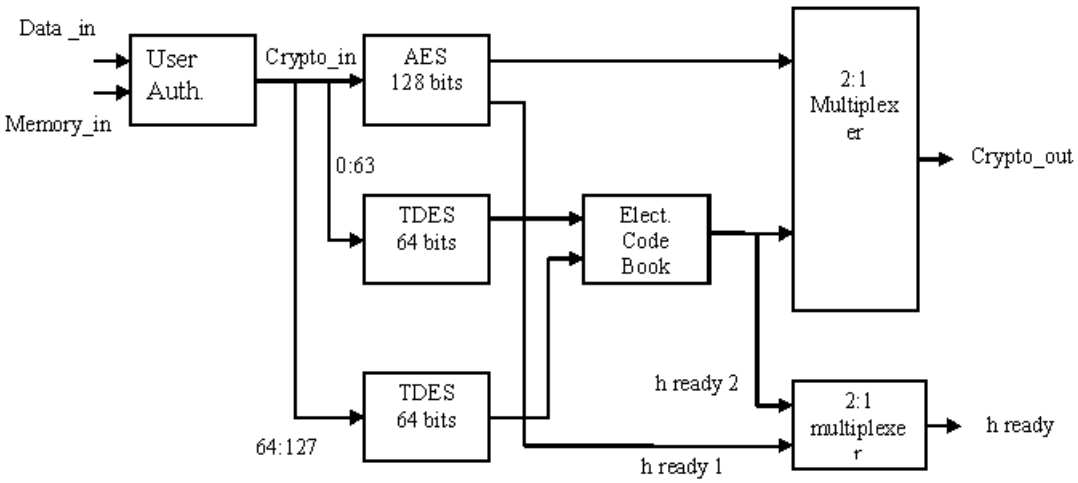

Figure 1: User Authentication Mode

required if AES and TDES are devised separately for comparison. Also a timestamp which is written C language is used to sort the edges of vertex.

The various tools used for implementation are:

- **Verilog**: Verilog is an enhanced platform of VHDL and design electronic circuits at multiple levels of abstraction. The modules of Verilog that could be realized physically are constructed in the form of RTL using synthesizable coding style. Verilog source is transformed into a netlist which is a logically equivalent description that consists of primary logic primitives available in FPGA and VLSI technology. The entire algorithm has been implemented in Verilog HDL.

- **Simulation Tools**:
  a) ICARUS Verilog: This is a synthesis and simulation tool that functions as a compiler for source code into the required target format. The main target of this tool is the simulation environment in Linux OS though it is compatible with many windows and MAC OS simultaneously.
  b) GTKWave: GTKWave is an offline analysis tool that debugs the error in Verilog programs. GTKWave is also a waveform analyzer that is primarily employed for the purpose of visualization.
  c) Make Utility: The primary objective of make tool is to generate executable programs and libraries automatically from the source code.

- **Synthesis Tools**:
  a) Xilinx ISE: This tool permits the designer to synthesize and compile their designs. The developers can also perform timing analysis, inspect RTL view, simulate a design reaction to different stimuli and configure target device according to the needs of the programmer.
  b) Cadence RTL Compiler and EDI System is a tool used for performance maximization with minimal area and power.
  c) Synopsys Design Vision: This tool takes HDL design to synthesize gate level HDL netlists.

4 Simulation Results and Analysis

A layout of crypto core and g-SIS implementation is generated in Cadence Encounter for TSMC 65nm technology. Figures 2, 3 and 4 display the waveforms, schematic and GDS II of AES algorithm. Here, the clock cycles are triggered for every 20 ns. A 32 bit hexadecimal input is fed into the system at the positive edge of the clock cycle. Both the key and the input are of the same length.

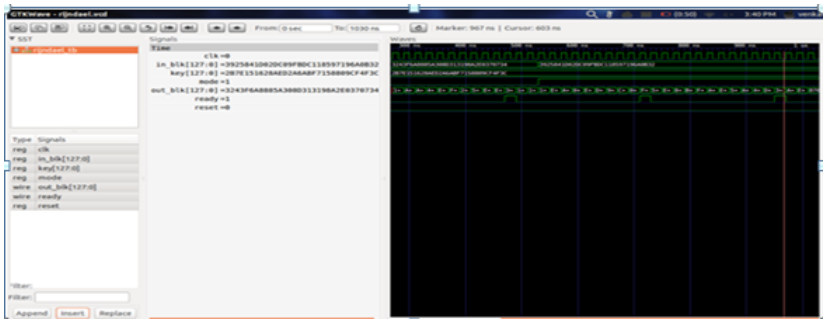

Figure 2: Waveforms of AES algorithm

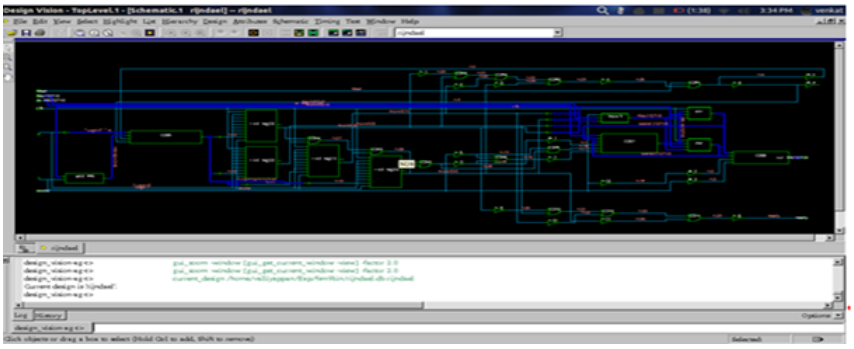

Figure 3: Schematic of AES algorithm

The output of AES was obtained by GTKWave analysis on every positive edge of the clock cycle.

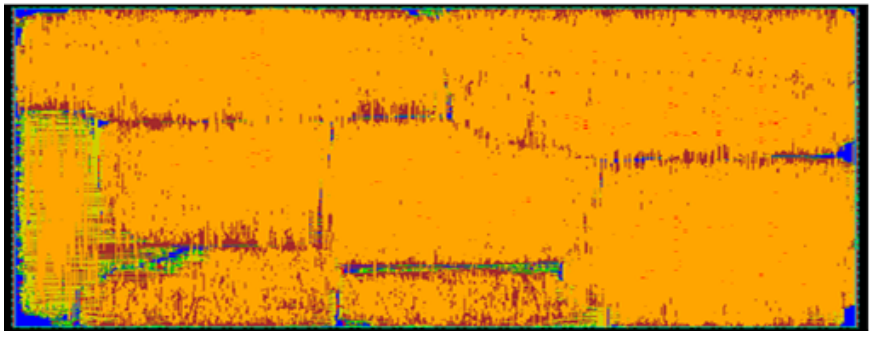

Figure 4: GDS II of AES algorithm

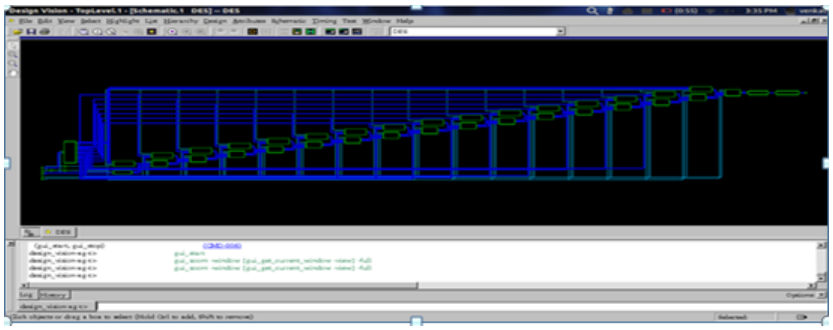

Figure 5: Schematic representation of DES algorithm

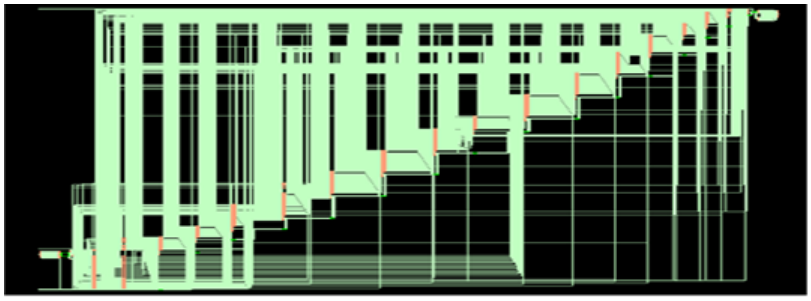

Figure 6: Schematic representation of DES algorithm

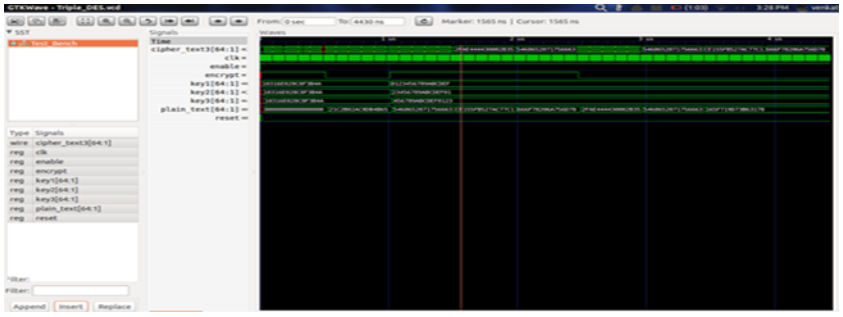

Figure 7: Waveforms of TDES algorithm

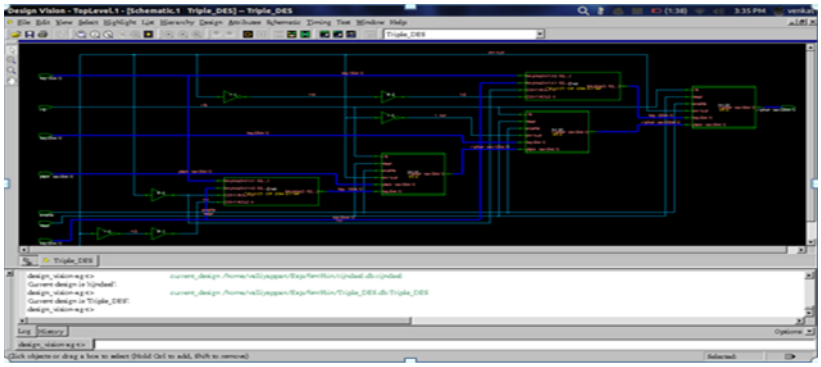

Figure 8: Schematic representation of TDES algorithm

In order to implement Triple DES, we need to instantiate three DES modules. Figures 5 and 6 give a schematic representation of the DES algorithm. The two Triple DES algorithms are implemented in a

Electronic Codebook approach. Figures 7 , 8 , 9 and 10 are the waveforms, schematics and GDS II for TDES algorithm.

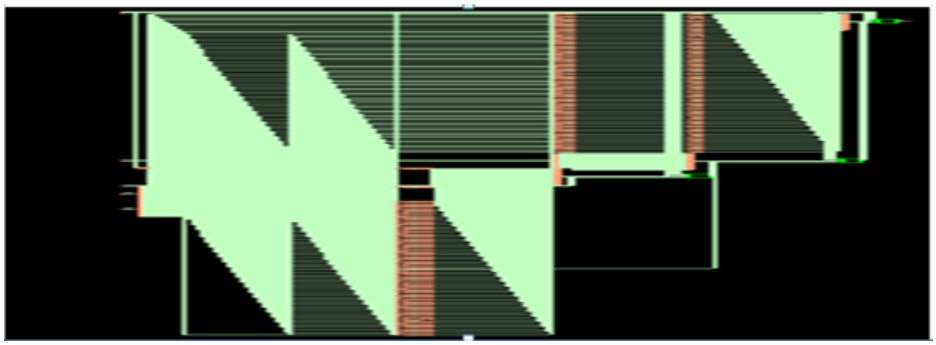

Figure 9: Schematic representation of TDES algorithm

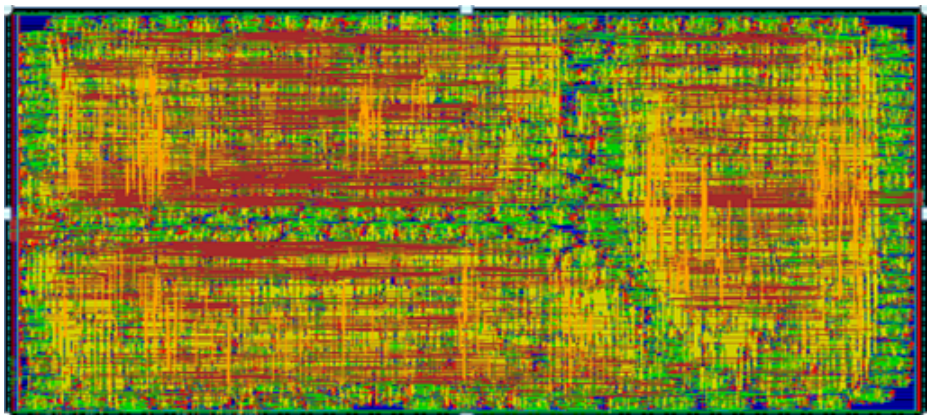

Figure 10: GDS II layout of TDES algorithm

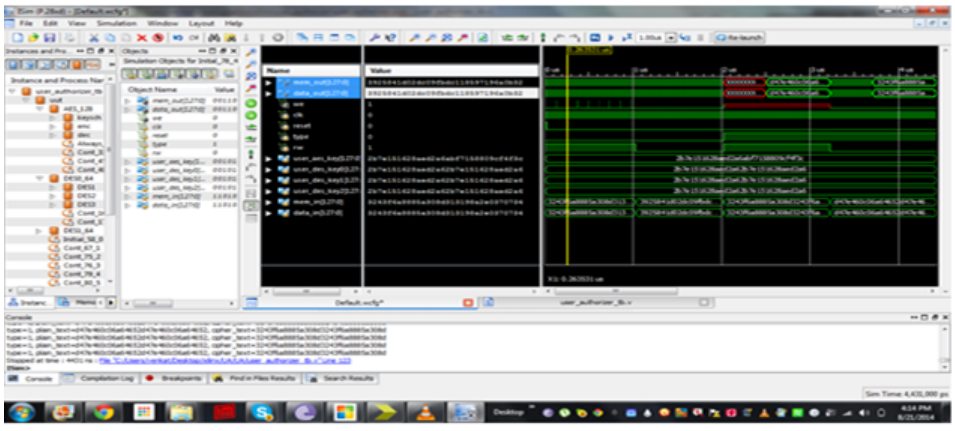

Figure 11: waveforms of g-SIS algorithm

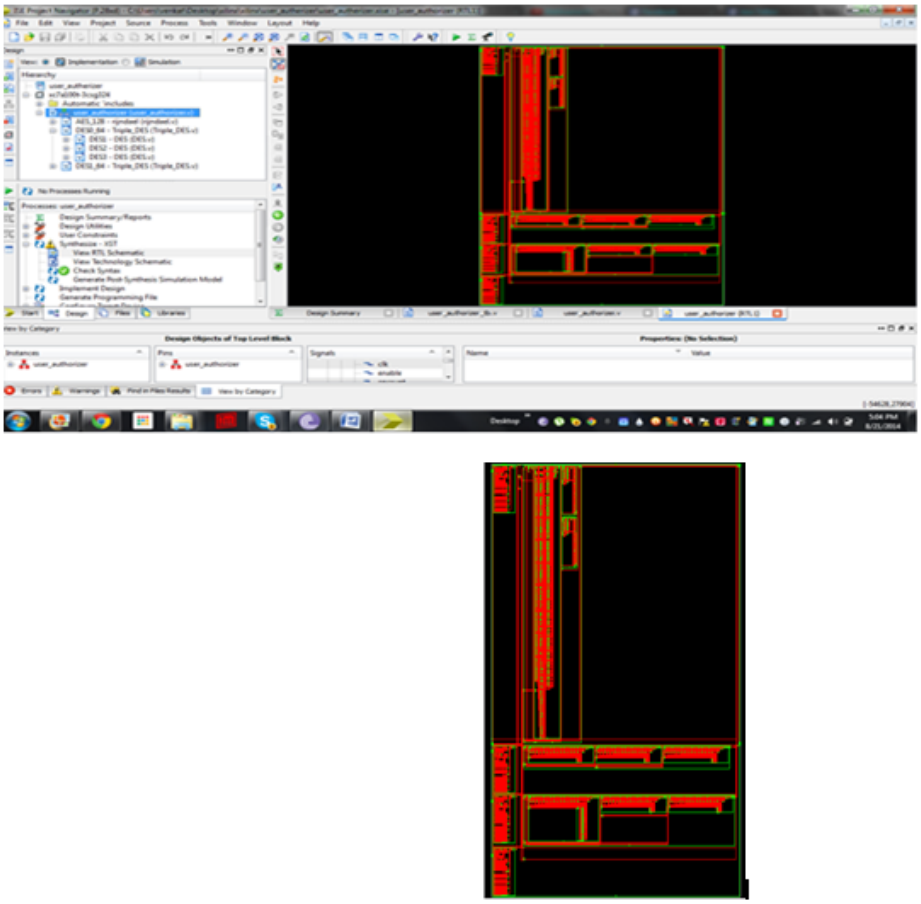

Figure 12: Schematic representation of g-SIS algorithm

Figure 11 shows the waveforms for g-SIS. In figure 12, the first longer blocks represent the implementation of AES algorithm along with its encrypt, decrypt and key schedule blocks. The following broader blocks represent the 64 bit LSB of TDES, including all its sub modules. Finally, the last broader blocks represent the 64 bit MSB of TDES. The GDS II layout of g-SIS algorithm is illustrated in figure 13.

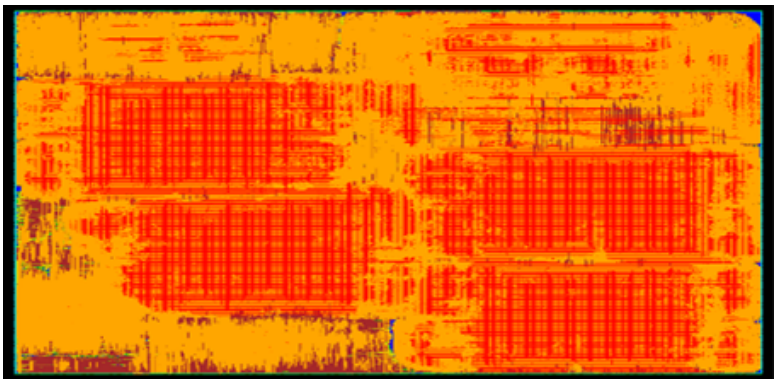

Figure 13: GDS II layout of g-SIS algorithm

Tables 1 and 2 give a comparative analysis between AES, TDES, DES and g-SIS algorithms in terms of area, number of cells, leakage power, dynamic power and total power. From the analysis, we can state that TDES possesses better values for area and power. Hence, it is recommended to be the first choice for the group centric sharing technique.

Instance	Cell	Cell Area
User Authorized	1459224	24802846
AES	1371901	23206796
TDES	42912	786687
DES	14229	261355

Table 1: Comparative Study of Area (Nanometer) for Various Algorithms

Modules	Cells	Leakage Power (nw)	Dynamic Power (nw)	Total Power (nw)
User Authorized	1459224	478826.581	100880649.107	101359475.688
AES	1371901	435871.46	89703738.778	40139610.243
TDES	42912	21169.714	29988148.450	30009318.164
DES	14229	7042.028	13113910.486	13120952.525

Table 2: Power Comparison of various Algorithms (Nano-Watt)

5 Conclusion

In this paper, the implementation of AES, DES and TDES algorithms is studied, tested and evaluated on 128 bits in terms of area and power. Apart from that, a comparative analysis of these algorithms is made and TDES is recommended to be the first choice for group centric secure information sharing model. Also, in order to match TDES with the 128 bits of AES algorithm, the TDES was instantiated twice in a parallel approach, i.e. the 64 bit LSB was ciphered by the first DES and the 64 bit MSB was ciphered by the second DES. A time stamp is also added to validate the objects precisely to their time accessed. The time stamp provides necessary information about the latest text and is also useful in cases where a minor upgrade of data is employed (example for release of new software version). Hence, we can state that both the AES and TDES algorithms can be simultaneously implemented in a single system, making it feasible for a wide range of applications.

References

[1] E. Agrawal and P. Pal. Refined polygram substitution cipher method: A enhanced tool for security. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(1):32–36, July 2012.

[2] K. T. Akashi Satoh, Sumio Morioka and S. Munetoh. A compact rijndael hardware architecture with s-box optimization. In *Proc. of the 7th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'01), Gold Coast, Australia*, volume 2248 of *Lecture Notes in Computer Science*, pages 239–254, December 2001.

[3] E. J. Alexandra Camacho and R. Krishnan. Design and low power vlsi implementation of triple-des algorithm. In *Proc. of the 2012 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP'12), Las Vegas, NV, USA*, pages 16–19, July 2012.

[4] T. M. .Cover and A. A. E. Gama. Capacity theorems for relay channel. IT-25(5):572–84, September 1979.

[5] T. Good and M. Benaissa. Very small fpga application-specific instruction processor for aes. *IEEE Transactions on Circuits and Systems – I: Regular Papers*, 53(7):1477–1486, July 2006.

[6] R. Krishnan, J. Niu, R. Sandhu, and W. Winsborough. Group-centric secure information sharing models for isolated groups. *ACM Transactions on Information and System Security (TISSEC)*, 14(3):1–29, 2011.

[7] N. B. of Standards. Data encryption standard (des). US Department of Commerce. Federal Information Processing Standards Publication 46 (FIPS PUB 46), January 1977.

[8] Y. Xiao, B. Sun, H.-H. Chen, S. Guizani, and R. Wang. Performance analysis of advanced encryption standard (aes). In *Proc. of the 2006 IEEE Global Telecommunications Conference (Globecom'06), San Francisco, CA, USA*. IEEE, November-December 2006.

[9] X. Zhang and K. K. Parhi. High-speed vlsi architectures for the aes algorithm. *IEEE Transactions on Very Large Scale Integration(VLSI) Systems*, 12(9):957–967, September 2004.

Author Biography

Eugene B John received a Ph.D from Pennsylvania State University. Currently he is Professor of Electrical and Computer Engineering at UTSA. His areas of research interests are Low Power VLSI Design, Computer Performance Evaluation, Cloud Benchmarking, Computer Architectures, Power-Aware and Reliable Systems.

Ram Krishnan received a Ph.D from George Mason University in 2010. He is currently an Assistant Professor of Electrical and Computer Engineering at UTSA. His area of research interest is computer and network security–specifically, access control (models and analysis) and security issues in cloud computing.

Valliyappan Valliyappan received his Bachelor's degree in Electronics and Communications Engineering from Anna University and a Master's degree in Electrical and Computer Engineering from UTSA. His area of research interest include Low power ASIC design and Verification, Digital VLSI design, and Computer architecture.

Sruthi Nanduru received her Bachelor's degree in Electrical and Electronics Engineering from JNTU. She is presently pursuing a master's in Electrical and Computer Engineering at UTSA. Her areas of research interest are Low Power VLSI Design and Computer Architecture.