JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5068-5077
https://publishoa.com
ISSN: 1309-3452

High Performance Using AES Algorithm in Cryptographic Application with Large 256-Bit Data Input

Dr. Malarkhodi S [1], Dr. Kavitha K [2]

Department of Electronics and Communication Engineering
[1] KS Rangasamy College of Technology, Tiruchengode, Tamilnadu, India
[2] VSB Engineering College, Karur, Tamilnadu, India
malarkhodi@ksrct.ac.in
kavitabala12@gmail.com

ABSTRACT

Cryptography is very important now-a-days for data security and integrity as the ecommerce and internet applications has increased. But, it has least importance in many cases because of extra memory and other requirements needed for the implementation. The main aim of this work is to implement Advanced Encryption Standard (AES) Encryption using Verilog. To protect data like electronics, cryptographic algorithms are used. The digital information can be encrypted and decrypted by the block cipher of AES algorithm. It can be implemented with the key length 128, 192, 256 bits. Each round of encryption associated with delay can be reduced by AES parallel design. For storing plain text, keys, and intermediate data, we construct two specific register banks, Key-Register and State-Register. Shift-Rows are inserted into the State- Register to save space. We build an efficient 8-bit block for Mix-Columns with four internal registers that take 8-bit and send out 8-bit to adapt the Mix-Column to an 8-bit data stream. For the key expansion and encryption phases, shared optimized Sub-Bytes are also used. We consolidate and simplify various Sub-Bytes to make them more efficient. The clock gating method is used in the design to decrease power consumption. This study provides a 256-bit AES architecture based on Image Cryptography. This design is built-in Verilog HDL on an FPGA XC3S 200 TQ-144, simulated using Modalism 6.4 c, and synthesized with the Xilinx tool.

Keywords— Advanced encryption standard (AES) algorithm, Clock gating, 256-bit data, Cryptography.

I. INTRODUCTION

Human being from ages had two inherent needs − (a) to communicate and share information and (b) to communicate selectively. These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand. The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. The word 'cryptography' was coined by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing. The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow. The features of AES are as follows.

Symmetric key symmetric block cipher

- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details

- Software implementable in HDL

Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, 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.

II. RELATED WORKS

Power analysis: A serious threat for FPGA security, M. Masoumi, Int. J. Internet Technol. Secured Trans., vol. 4, no. 1, pp. 12–25, Differential power analysis (DPA) [11] attack and also illustrates a practical and successful implementation of this attack against an FPGA implementation of the AES algorithm. , Differential power analysis (DPA) attack and also illustrates a practical and successful implementation of this attack against an FPGA implementation of the AES algorithm. The research of DPA attacks against AES implementations
H. Yu, Z. Xue-Cheng, L. Zheng-Lin, and C. Yi-Chen, J. China Univ. Posts Telecommun. vol. 15, no. 4, pp. 101–106, [7]
A simulation-based experimental environment is built to acquire power data, and single-bit differential power analysis (DPA), and multi-bit DPA and correlation power analysis (CPA) attacks are conducted. AES against first and second-order differential power analysis Applied Cryptography and Network Security. J. Zhou and M. Yung, Eds. vol. 6123, Springer-Verlag, pp. 168–185. Berlin, Germany, Differential Power Analysis (DPA) [8] is a powerful and practical technique used to attack a cryptographic implementation in a resource limited application environment. High-speed VLSI architectures for the AES algorithm, X. Zhang and K. K. Parhi, IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 12, no. 9, pp. 957–967, High-speed architectures for the hardware implementation of the Advanced Encryption Standard (AES) algorithm [14].

III. PROPOSED NANO AES DESIGN

A lightweight AES architecture for different applications is designed including resource-constrained IoT application. The design has 8-bit data path and including two specified register banks for storing plain text, keys, and intermediate results. To reduce the required logic, Shift-Rows were designed to run inside of the State-Register.

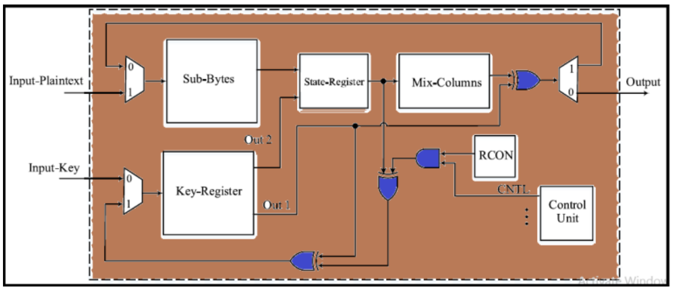


Fig 1. Modified Nano AES Encryption

The AES implementation consists of the Core AES core and Clock gating to generate the encryption masks. The proposed AES core can perform both 128 bit and 256 bit encryption. The process is done in 10 cycles by using 128 bit key, computing 1 round per cycle, with the hardware of each round being reused to save area verses a fully unrolled implementation. The proposed nano AES is shown above in figure 1 and figure 2. Where the original data (plaintext) is first nano by a random mask. The nano plaintext and the mask are, then, fed through the "Nano AES core" which encrypts the nano data with the secret key. Result nano cipher-text is given as input into the module to arrive at the intended cipher-text.

1) The Shift-Rows are embedded inside the State-Register in order to reduce the required logic.

2) The Sub-Byte blocks are optimized and shared with both key expansion phase and encryption phase.

3) An optimized 8-bit block is designed for Mix-Columns with 8-bit input and output that is based on the structure of 8-bit data path, which is followed by Add-Round-Key. Thus, the results are sent to Add-Round-Key byte-by-byte. In comparison to 32-bit Mix-columns, it is not necessary to store the results in the registers or increase the data path for Key-Register to 32-bit.

4) The clock gating technique is applied in different parts of the design in order to reduce the power consumption of the design.

The modified architecture is shown in figure 1. In the different parts of the design, we apply the clock gating technique to reduce the dynamic power consumption. The clock gating is separately applied on State-Register, the internal registers of Mix-Columns, Key-Register, and RCON. The most power consumption is saved during the key expansion phase for instance. The clock of State-Register and Mix- Columns is disabled to save power as because these two blocks are not used in the key expansion phase.

This Decryption Process is done by inv mixed Column, inv Sub bytes. The modified Nano AES decryption is shown in figure 2.

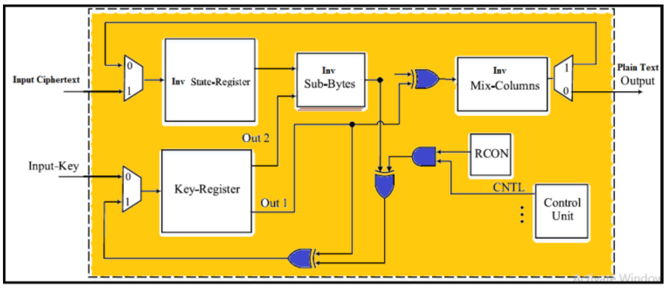


Fig 2. Modified Nano AES Decryption

CLOCK GATING:

Clock gating is a well-known technique to reduce chip dynamic power. Recent clock gating techniques based on ACG (Adaptive Clock Gating) and instruction level clock gating. clock gating technique reduces not only switching activity of functional blocks in IDLE state but also dynamic power in running state. Our modified ACG (Adaptive Clock Gating) can automatically enable or disable the clock of the functional block. Clock gating is a popular technique used in many synchronous circuits for reducing dynamic power dissipation. Clock gating saves power by adding more logic to a circuit to prune the clock tree. This technique is shown in figure 3.

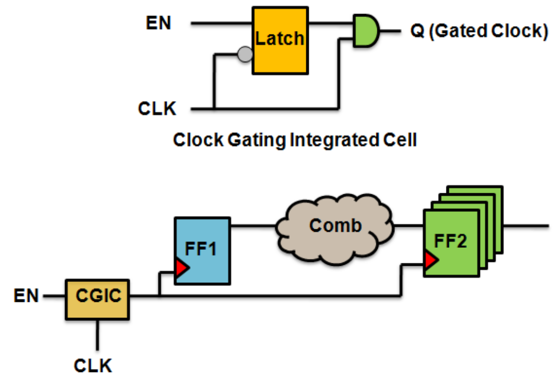


Fig 3. Clock Gating Technique

Everywhere acceptance of portable devices such as cell phones, PDAs and mp3 players has much research in the development of technique for low-power design. The continuous decrease in the minimum feature size of transistors which increase of both device density and design complexity. The overall power dissipation on a chip is due to clock and data-path.

The clock -gating is one of the effective logics in RTL and architectural power reduction.

Clock gating is an effective technique to reduce dynamic power, because individual IP usage varies across applications, not all IP cores are used all the time, giving rise to opportunity for reducing the unused IP cores' power. By combining (AND gate) the clock with a gate-control signal, clock gating essentially disables the clock to an IP core when that IP is not used, avoiding power dissipation due to unnecessary charging and discharging of the unused circuits.

The clock -gating is one of the effective logic in RTL and architectural power reduction. Clock gating is an effective technique to reduce dynamic power. We will design decryption scheme based on Proposed Scheme.

256-BIT DATA ENCRYPTION:

In this 256-bit data is taken as input and then divided into two 128-bit data. Next the 128-bit data is encrypted and decrypted using AES algorithm. The final output of 256 bit is taken from the two decrypted data as shown below in figure 4 and figure 4.1.

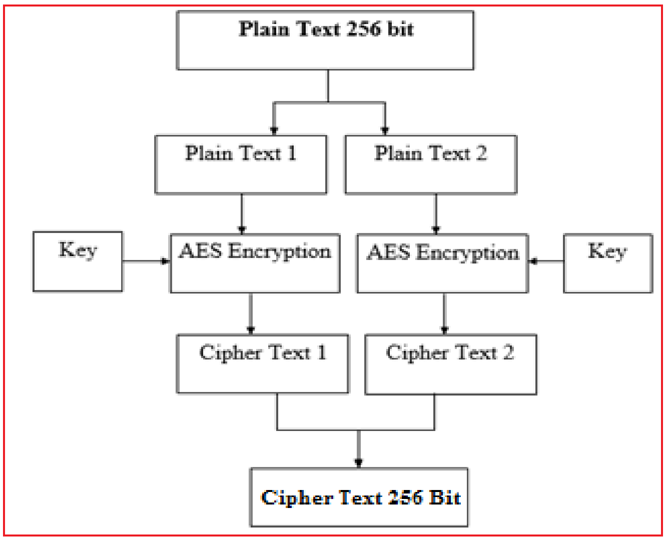


Fig 4. 256-bit data encryption block diagram

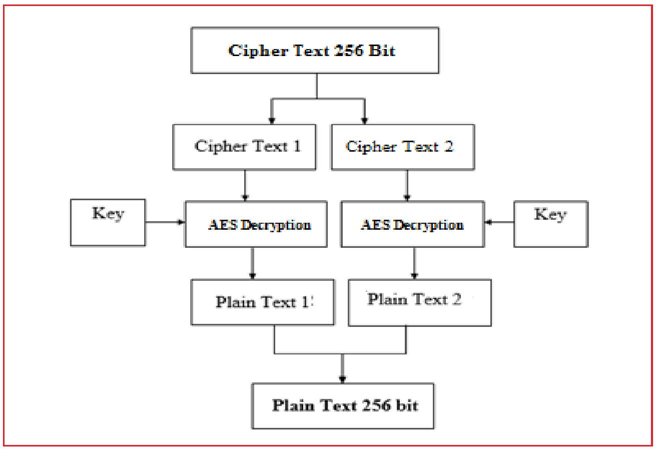
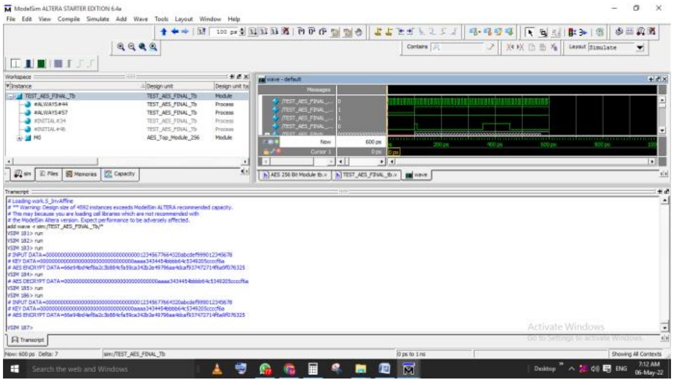


Fig 4.1 256-bit data decryption block diagram

V. SIMULATION RESULTS

The simulation results are shown below in figures 5.1 and 5.2 for 256-bit data encryption and decryption by designing two separate 128-bit data encryption and decryption. The simulation is done using 256 bit data using hexadecimal, decimal and text messages as inputs. The same process for 128-bir data encryption is done for two 128-bit data and processed for 256-bit data. The RTL view of the design is shown in figures 6.1 and 6.2.



```
# Loading work.S_InvAffine
# ** Warning: Design size of 4592 instances exceeds ModelSim ALTERA recommended capacity.
# This may because you are loading cell libraries which are not recommended with
# the ModelSim Altera version. Expect performance to be adversely affected.
add wave -r sim:/TEST_AES_FINAL_Tb/*
VSIM 181> run
VSIM 182> run
VSIM 183> run
# INPUT DATA =0000000000000000000000000000000012345677664320abcdef999012345678
# KEY DATA =00000000000000000000000000000000aaaa34344454bbbb64c5349205ccccf6a
# AES ENCRYPT DATA =66e94bd4ef8a2c3b884cfa59ca342b2e49796aa4dcaf937472714f6a9f076325
VSIM 184> run
# AES DECRYPT DATA =00000000000000000000000000000000aaaa34344454bbbb64c5349205ccccf6a
VSIM 185> run
VSIM 186> run
# INPUT DATA =0000000000000000000000000000000012345677664320abcdef999012345678
# KEY DATA =00000000000000000000000000000000aaaa34344454bbbb64c5349205ccccf6a
# AES ENCRYPT DATA =66e94bd4ef8a2c3b884cfa59ca342b2e49796aa4dcaf937472714f6a9f076325

VSIM 187>
```

Fig 5.1 256-bit data encryption and decryption

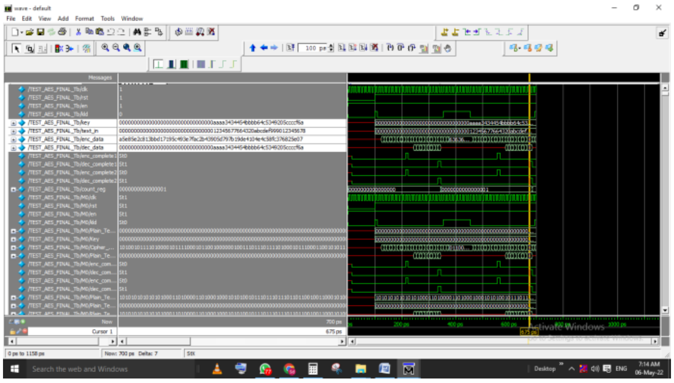


Fig 5.2 256-bit data encryption and decryption

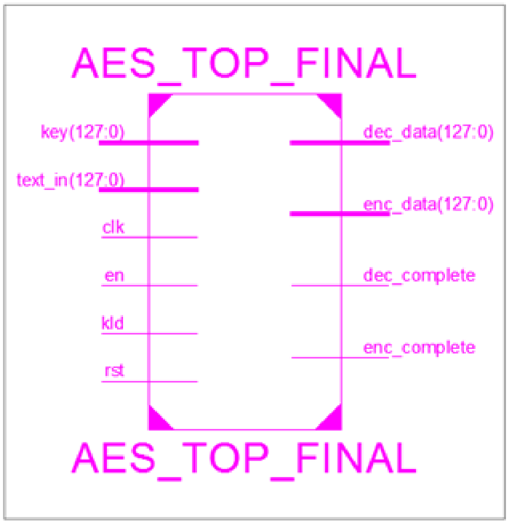


Fig 6.1 RTL View of AES MAIN Module

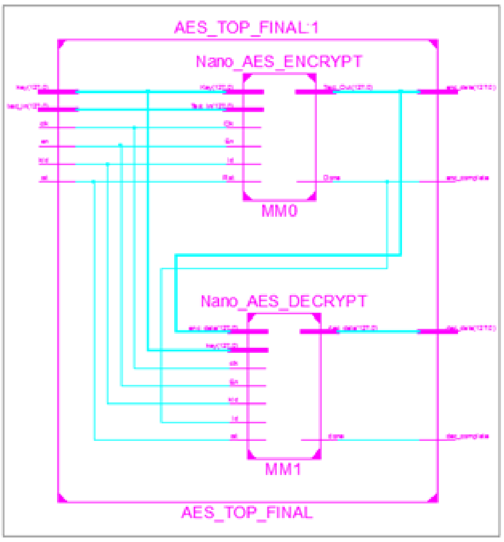


Fig 6.2 RTL View of AES Module

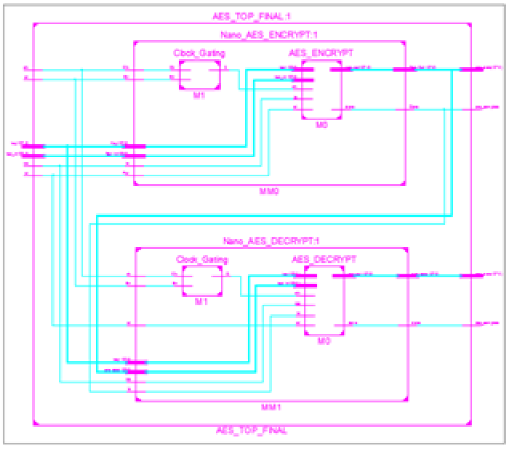


Fig 6.2. Inner View of TOP AES design

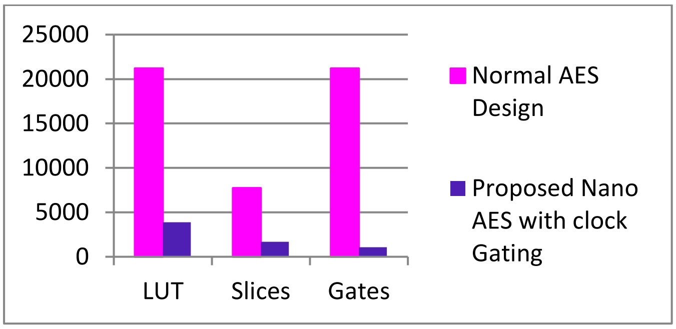
VI. COMPARISON AND ANALYSES

The proposed design is synthesized using Xilinx for different bit sizes and the delay and area have been analyzed for comparison.

Table 1 Comparison of existing and proposed model

From the table 1, it is observed that AES Design with clock gating has minimum area and it becomes lesser delay compared to AES as the number of bits. The results show that the use of clock gating in AES for addition achieves overall minimum area and delay in the proposed design. The comparison chart is drawn as shown in figures 7.1 and 7.2 for area analysis and delay analysis.

Comparison Chart



Method Name	Area			Delay in ns		
	Slice	Register	LUT	Max Delay	Gate Delay	Path Delay
Normal AES Design	**7734**	**21207**	**21207**	**160.860**	**25.302**	**135.558**
Proposed Nano AES with Clock Gating	**1670**	**1066**	**3900**	**3.405**	**2.923**	**0.482**

Fig 7.1. Area Analysis

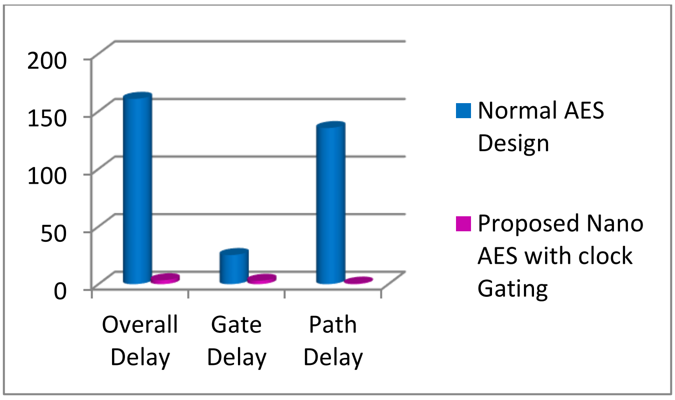
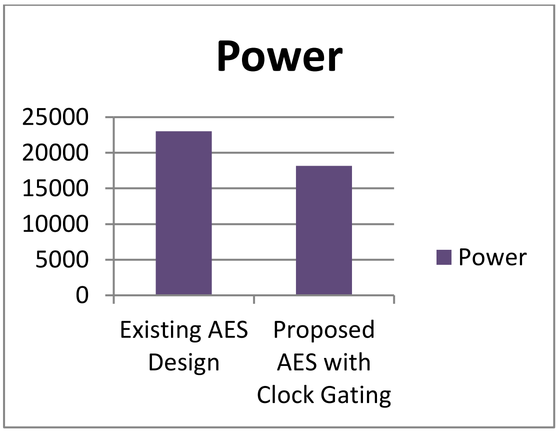


Fig 7.2. Delay Analysis

Table 2 Comparison of existing and proposed model

From the comparison table 2, the power analysis is done for the existing system and the proposed model with clock gating technique and found that the power consumption is reduced. The comparison chart is drawn for the above data and shown in figure 7.3.

METHOD NAME	POWER
Spartan XC3s5000-4fg1156	**TOTAL POWER (mW)**
Existing AES Design	**23032**
Proposed AES with Clock Gating	**18155**



7.3 Power Analysis

VII. APPLICATION

Image Cryptography

The AES algorithm is used effectively with image input and simulated using MATLAB for the conversion of image into plain text and the plain text is encrypted and then decryption is done for the plain text. The final output image is retrieved using MATLAB as shown below in figures 8.1, 8.2 and 8.3 for the given image input respectively.

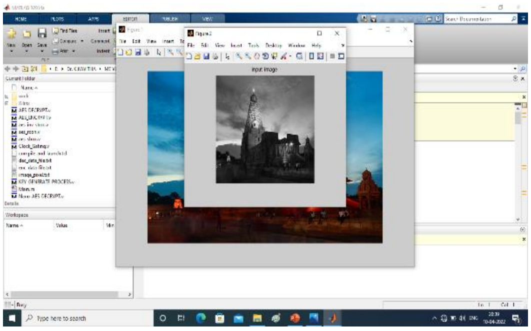


Fig. 8.1 Image input

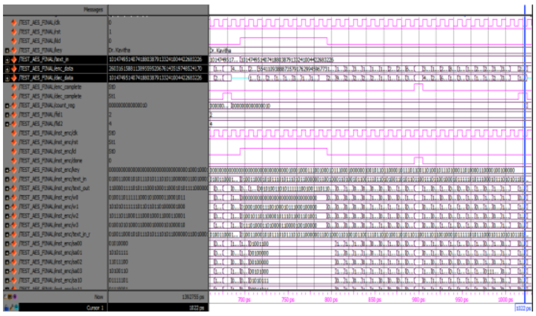
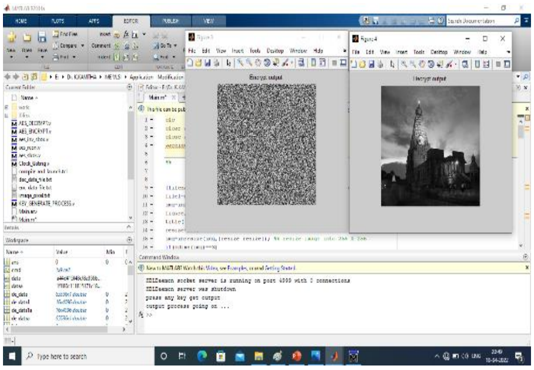


Fig. 8.2 Image input into plain text



```
SDLDaemon socket server is running on port 4999 with 0 connections
SDLDaemon server was shutdown
press any key get output
output process going on ...
>>
```

Fig. 8.3 Image output

VIII. CONCLUSION

AES algorithm is a secure symmetric cryptography algorithm with a high level of security, which is widely used in many applications and networks. The 256-bit data input is encrypted and decrypted using the 128-bit key and simulated. The design had 8-bit data path and included two specified register banks for storing plain text, keys, and intermediate results. To reduce the required logic, the different blocks used are optimized and hence reduced the area, delay and power consumption by using the clock gating technique in different blocks of the design. The results are compared between the normal AES design and the proposed design and found that the area and delay are reduced due to the optimization. Also the power analysis is done and found that the power consumption is reduced due to clock gating. This design is simulated by Modelsim 6.4 c and Synthesized by Xilinx tool and found that the performance of the proposed design is high compared with the normal AES algorithm.

REFERENCES

[1] A. Shreedhar, K.-S. Chong, N. K. Z. Lwin, N. A. Kyaw, L. Nalangilli, W. Shu, J. S. Chang, and B.-H. Gwee, 2019, “Low Gate-Count Ultra-Small Area Nano Advanced Encryption Standard (AES) Design”, IEEE International Symposium on Circuits and Systems (ISCAS)

[2] Ali Akbar Pammu, Weng-Geng Ho, Ne Kyaw Zwa Lwin, Kwen-Siong Chong and Bah-Hwee Gwee, 2018, “A High Throughput and Secure Authentication-Encryption AES-CCM Algorithm on Asynchronous Multicore Processor”, IEEE Transactions on Information Forensics and Security PP(99)

[3] Arash Reyhani-Masoleh, Mostafa Taha and Doaa Ashmawy, 2018, “New Area Record for the AES Combined S-box/Inverse S-box”,

[4] D. Gu, J. Li, S. Li, Z. Ma, Z. Guo, and J. Liu, 2012, “Differential fault analysis on lightweight block ciphers with statistical cryptanalysis techniques”, Fault Diagnosis and Tolerance in Cryptography (FDTC)

[5] Ho Keun Kim1&Myung Hoon Sunwoo, 2019, “Low Power AES Using 8-Bit and 32-Bit Data path Optimization for Small Internet-of-Things (IoT)”, Journal of Signal Processing Systems.

[6] Hossein Kouzehgar, Meisam Nesary Moghadam and Pooya Torkzadeh, 2018, “A High Data Rate Pipelined Architecture of AES Encryption/Decryption in Storage Area Networks”, 26th Iranian Conference on Electrical Engineering (ICEE2018)

[7] H. Yu, Z. Xue-Cheng, L. Zheng-Lin, and C. Yi-Chen, 2008, “The research of DPA attacks against AES implementations”, J. China Univ. Posts Telecommun. vol. 15, no. 4, pp. 101–106

[8] J. Zhou and M. Yung, Eds, 2010, “AES against first and second-order differential power analysis Applied Cryptography and Network Security”, Springer-Verlag, Berlin, Germany, vol. 6123, pp. 168–185

[10] Karim Shahbazi, Seok-Bum Ko, 2019, “High throughput and area-efficient FPGA implementation of AES for high-traffic applications”, IET Computers & Digital Techniques

[11] M. Masoumi, 2012, “Differential power analysis: A serious threat for FPGA security”, Int. J. Internet Technol. Secured Trans., vol. 4, no. 1, pp. 12–25

[12] Sa’ed Abed, Reem Jaffal , Bassam Jamil Mohd and Mohammad Alshayeji, 2019, “FPGA Modelling and Optimization of a SIMON Lightweight Block Cipher” Journal sensors

[13] Shahriar Ebrahimi, Siavash Bayat-Sarmadi, Hatameh Mosanaei-Boorani, 2019, “Post-Quantum Crypto processors Optimized for Edge and Resource-Constrained Devices in IoT”, IEEE Internet of Things Journal PP(99):1-1

[14] X. Zhang and K. K. Parhi, 2004, “High-speed VLSI architectures for the AES algorithm”, IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 12, no. 9, pp. 957–967

[15] Zhe Liu, Kim-Kwang Raymond Choo, and Johann Großschädl, 2019, “Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography”, IEEE Communications Magazine