iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.46613

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

Image Cryptography Design Based on Nano AES Security Algorithm

Varsha. P, Dr. V. Nanammal [2]
[1]*M.E Student,* [2]*Assistant professor, Deportment of Electronics and Communication Engineering, Jeppiaar Engineering College, Chennai - 600 119,India*

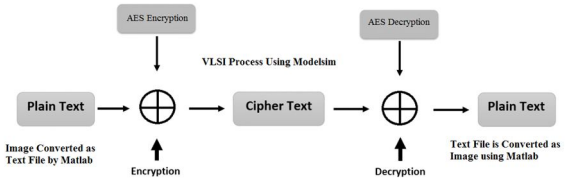
Abstract: ***Advanced Encryption Standard (AES) is a specification for electronic data encryption. This standard has become one of the most widely used encryption methodand has been implemented in both software and hardware. A high-secure symmetric cryptography algorithm, implementation on field-programmable gate array (FPGA). The proposed architecture includes 8-bit data path and five main blocks. We design two specified register banks, Key-Register and State-Register, for storing the plain text, keys, and intermediate data. To reduce the area, Shift-Rows is embedded inside the State- Register. To optimize Sub-Bytes, we merge and simplify some parts of the Sub-Bytes. To reduce power consumption, we apply the clock gating technique to the design. This paper presents an Image Cryptography based 128-bit AES design. This Design is implemented in FPGA XC3S 200 TQ-144 using Verilog HDL and simulated by Modelsim 6.4 c and Synthesized by Xilinx tool.***

I. NTRODUCTION

Cryptography, 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 of encryption takes a clear-text document and applies a key and a mathematical algorithm to it, converting it into crypto-text. 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), a branch of the US government, started a process to identify a replacement for the Data Encryption Standard (DES). 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 Pipelined (derived from their names) for the algorithm. After adoption the encryption algorithm was given the name Advanced Encryption Standard (AES) 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). As expected, many providers of encryption software and hardware have incorporated AES encryption into their products.

II. CIRCUIT DESCRIPTION

We exploit the SDRR in a conventional advanced encryption standard (AES)-128architecture, improving the immunity of the cryptographic hardware to the state-of-the-art PAAs. In the AES-128 exploiting SDRR, the combinational path evaluates random data throughout the entire clock cycle, and the interleaved processing of random and real data ensures the protection of both combinational and sequential logics.



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

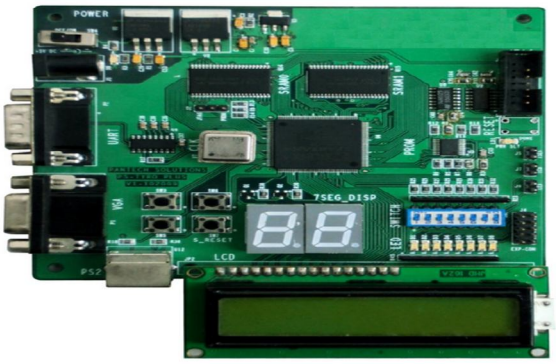
III. PRINCIPLE OF OPERATION

1) *Smaller Physical Size:* Smallness is often an advantage in itself—consider portable televisions or handheld cellular telephones.
2) *Lower Power Consumption:* Replacing a handful of standard parts with a single chip reduces total power consumption. Reducing power consumption has a ripple effect on the rest of the system: a smaller, cheaper power supply can be used; since less power consumption means less heat, a fan may no longer be necessary; a simpler cabinet with less shielding for electromagnetic shielding may be feasible, too.
3) *Reduced Cost:* Reducing the number of components, the power supply requirements, cabinet costs, and so on, will inevitably reduce system cost. The ripple effect of integration is such that the cost of a system built from custom ICs can be less, even though the individual ICs cost more than the standard parts they replace. Understanding why integrated circuit technology has such profound influence on the design of digital systems requires understanding both the technology of IC manufacturing and the economics of ICs and digital systems.

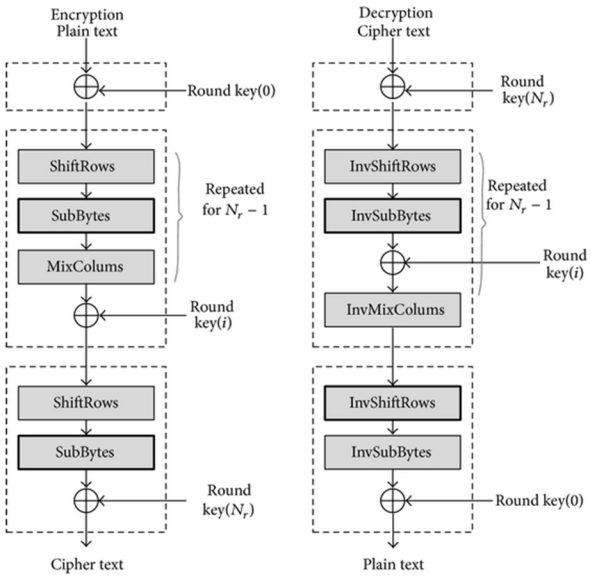
IV. COMPONENTS PLACEMENT

A. *Spartan 3 XC3S 200 TQ 144*

The Spartan-3 EDK Board provides a powerful, self-contained development platform for designs targeting the new Spartan-3 FPGA from Xilinx. It features a 200K gate Spartan-3, on-board I/O devices, and 1MB fast asynchronous SRAM, making it the perfect platform to experiment with any new design, from a simple logic circuit to an embedded processor core. The board also contains a Platform Flash JTAG-programmable ROM, so designs can easily be made non-volatile.

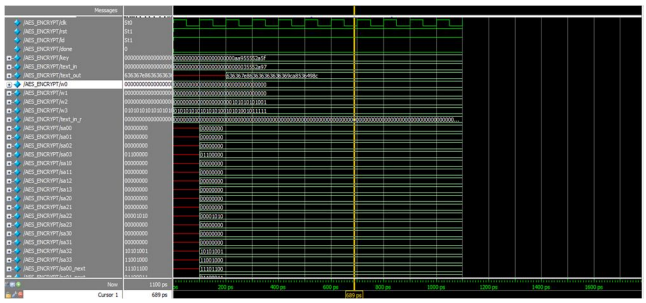


V. ENCRYPTIONPROCESS

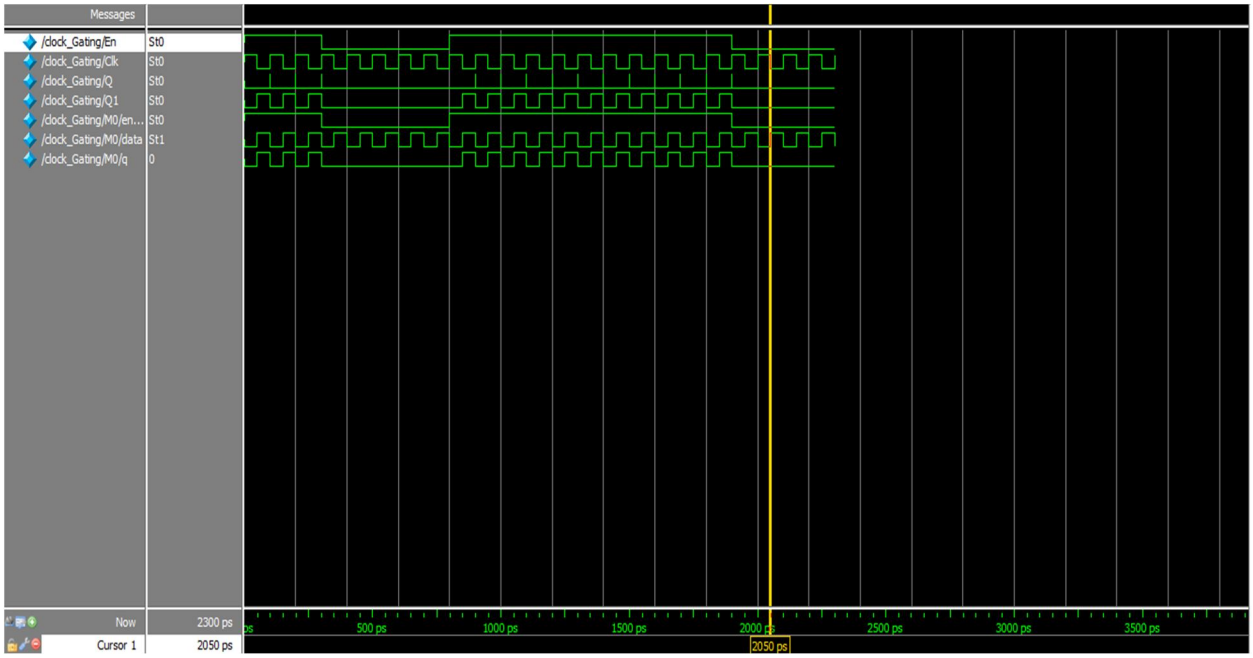


VI. RESULTS AND DISCUSSION

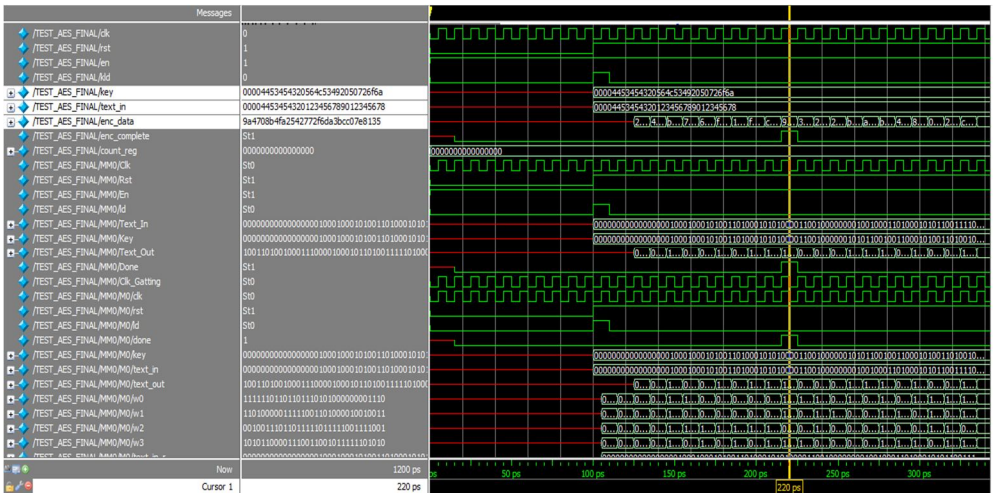
A. *AES Encryption*



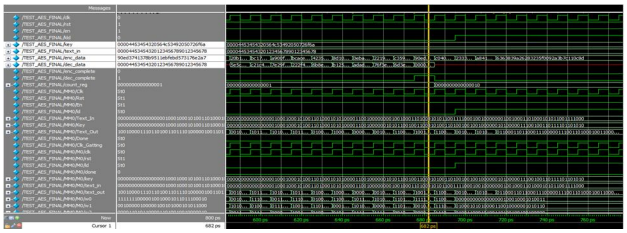
B. *Clock Gating*



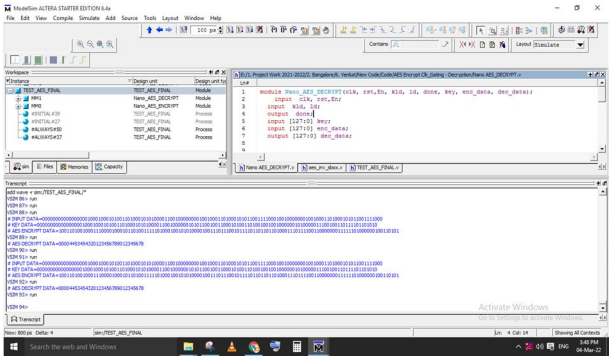
C. *Nano AES Clock Gating Encryption*



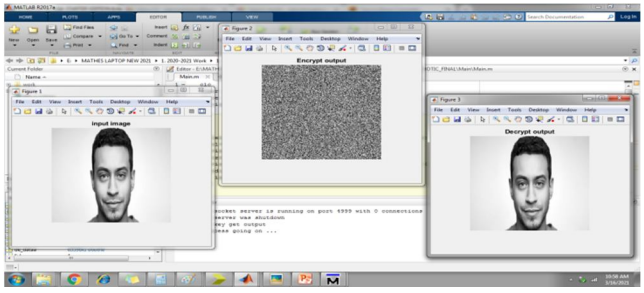
D. Nano AES Clockgating Encryption & Decryption



E. Nano AES Clock Gating Encryption & Decryption



F. Application Output

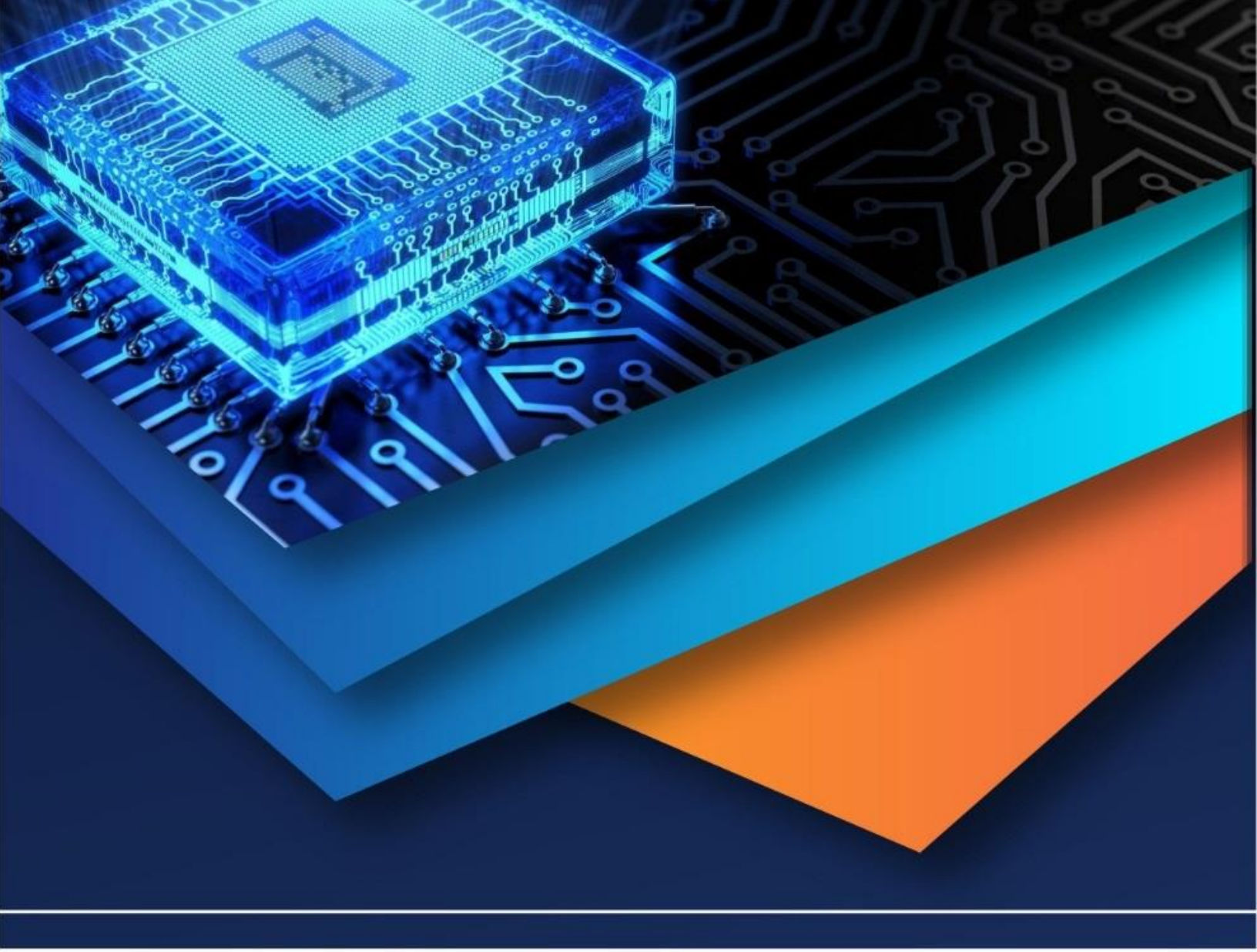


VII. CONCLUSION

Nano AES is a secure symmetric cryptography algorithm with a high level of security, which is widely used in many applications and networks. Thus, AES is a suitable algorithm for tiny IoT devices. In this article, we designed a lightweight AES architecture for resource-constrained IoT devices. The design had 8-bit datapath and included two specified register banks for storing plain text, keys, and intermediate results.

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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY