International Journal of Research in Engineering, Science and Management
Volume 5, Issue 6, June 2022
https://www.ijresm.com | ISSN (Online): 2581-5792

High Security and Low Power Nano AES Security Algorithm for Image Cryptography

G. D. Archana[1], H. Chandana[2], N. Sanjay[3*], P. Shashikumar[4], N. Vidyashree[5]
[1,2,3,4]*Student, Department of Electronics and Communication Engineering, East West Institute of Technology, Bangalore, India*
[5]*Professor, Department of Electronics and Communication Engineering, East West Institute of Technology, Bangalore, India*

***Abstract*: Advanced Encryption Standard (AES) is a type of data encryption. It is one of the most widely used encryption method and implemented in both software and hardware. On a field programmable gate array, this cryptographic technique is implemented (FPGA). The suggested design consists of five operating blocks and employs an 8-bit data channel. For the storage of plain text, keys, and intermediate data, we employ two types of registers: Key-Register and State-Register. Shift-Rows are insert-ed within the State-Register Mix-Columns to save space. They are constructed with four internal registers that take and return 8-bits. Optimized for sharing for the key expansion and encryption phases, sub-bytes are assigned. To reduce power consumption, we implement the clock gating technique in the design. This paper presents an Image Cryptography based 128-bit AES design. The Design will be implemented on FPGA XC3S 200 TQ-144 kit using Verilog HDL as programming language and its design is simulated by Modelsim 6.4 c. The synthesis process is done through Xilinx tool.**

***Keywords*: Cryptography, key register, State-Register clock gating technique.**

1. Introduction

Cryptography, is also known as encryption. It is the method of creating and using of cipher to protect the data while transmitting to a particular receiver from reading or using the information. cryptosystem is used to encode the information. Receiver can only view the encrypted information if he/she has corrected key and correct algorithm. The algorithm is primarily used while communicating important messages or important images. This procedure applies a key and suggested algorithm to a text document. The document is illegible in crypto-text until the recipient gets a key that can decrypt the cypher text. The encryption method submitted by Belgian cryptographers Joan Daeman and Vincent Rijmen was chosen by a unanimous vote. The method suggested by Joan Daeman and Vincent Rijmen was given the moniker Pipelined (taken from their names). After it was adopted, the encryption algorithm was given the name AES.

An AES encryption algorithm uses multiple rounds of encryption and an encryption key. Block ciphers are encryption algorithms that work on a single block of data. AES encryption uses a 128-bit block size. The term "rounds" refers to an encryption technique that combines data before re-encrypting it up to ten times. The length of the key determines how many times it may be encrypted. The AES algorithm encrypts data with a single key. 128-bit (16-byte), 192-bit (24-byte), or 256-bit keys are available (32 bytes). The usage of a 128-bit key is referred to as 128-bit encryption. Cipher keys are used in both encryption and decryption in AES. The symmetric encryption algorithm is the name given to this procedure. Asymmetric encryption techniques employ two keys: a public key and a private key. Encryption keys are data strings that are binary in nature and are used to encrypt data. The encryption key is the same for encrypting and decrypting data. The key is generated by software. A pass phrase is used to create a key. We will never utilise a pass phrase alone as a key in a decent encryption scheme.

2. Literature Survey

A. Survey Paper 1

Karim Shahbazi and Seok-Bum Ko published a paper "Area-Efficient Nano-AES Implementation for Internet-of-Things Devices" In which They had found that end-to-end security is vital for the devices which is connected to the IoT. They demonstrated a lightweight enhanced encryption standard based on an FPGA-implemented more secure cryptography algorithm. They suggested a five-block design with an 8-bit data route. For data storage, two register banks are defined, one for Key Register and the other for State Register.

3. Proposed Methodology

The Model consists of two phases:

1) *Encryption:*
   - First the input image will be converted into plain text by using matlab functions.
   - Then the input plain text is encrypted using AES algorithm.
   - The encrypted text is called cipher text.
2) *Decryption*
   - The cipher text is decrypted using AES algorithm.
   - After decryption cipher text is back to plain text.
   - The plain text is converted to image using matlab function.

*Corresponding author: san265jay@gmail.com

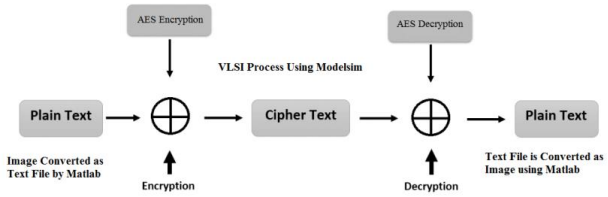

Fig. 1. Proposed system architecture

4. Requirements

A. *Software Requirements*

- MATLAB
- Modalism
- Xilinx ISE

B. *Hardware Requirements*

- Spartan 3XE 3S

5. Implementation

- To simplify the logic, the Shift Rows are contained into the State Register.
- The optimised Sub-Bytes block will be used in both the key expansion and encryption phases.
- Creating an 8-bit block for Mix Columns operation with an 8-bit input and output structure that is equivalent to an 8-bit data channel. The Add Round Key action comes after the Mix Columns procedure. Byte-by-byte, the results are sent to Add Round Key.
- The clock-gating approach is applied to the key register to lower the system's power consumption.
- Clock gating is a semiconductor dynamic power reduction approach.
- Switching activity is decreased by applying the clock gating approach, which decreases functional blocks in the idle state and dynamic power in the operating state.
- Our modified Adaptive Clock Gating technique can automatically enable or disable the clock.

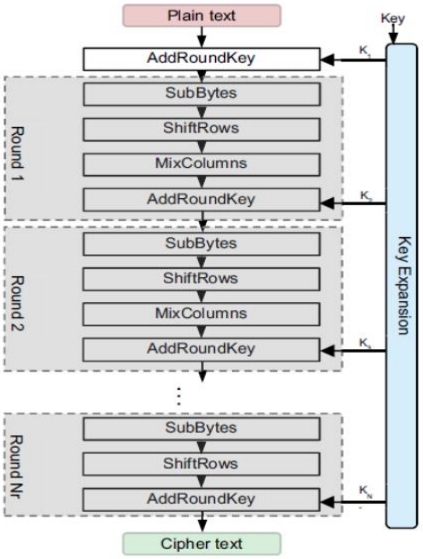

Fig. 2. Proposed algorithm

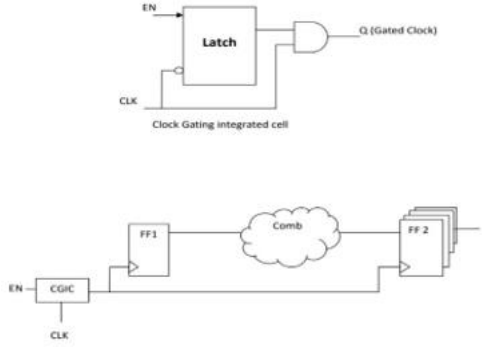

Fig. 3. Clock gating technique

6. System Outcomes

The proposed system includes three steps i.e., grey scale conversion, Encryption, decryption.

1) ***Grey scale conversion***

- First the input image will be converted into grey image by using matlab functions.
- Below shows the figure of color image converted into grey scale image.

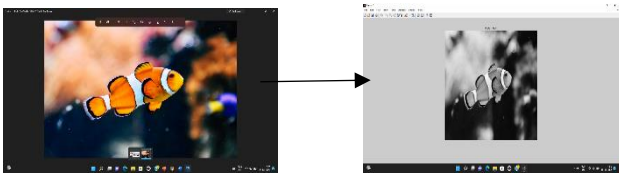

Fig. 4. Image converted from color to grey images

2) *Encryption*

Then the grey image is encrypted using AES algorithm.

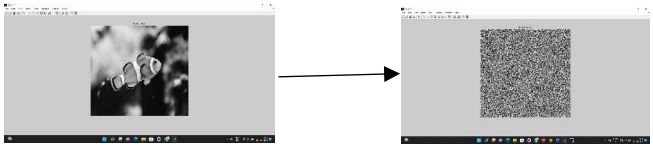

Fig. 5. Encryption of grey image

3) *Decryption*

The cipher text is decrypted using AES algorithm.

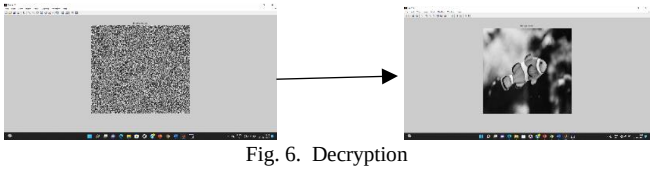

Fig. 6. Decryption

Advantages:

- It consumes Less power.
- It consumes Less energy and has high-throughput hardware by providing multiple levels.
- It has High security with Best Attack Prevention scheme.

Future enhancement:

- It can withstand against hacking attempts because it has higher length key sizes (128 bits).

- Since AES has initial permission secured, it remains highly accessible for both the private and public sectors.

7. Conclusion

The Nano AES algorithm is a symmetric encryption that is safe. It provides a high level of security and is utilized in a broad variety of applications and networks. The goal of building a lightweight AES architecture is to decrease the amount of logic required. The State-Register was used for the Shift-Rows procedure. The design includes an optimised Sub-Bytes phase that is shared with encryption and key expansion. We also created a block for mixing columns with 8-bit input and output. To save space and electricity, the clock gating approach was applied. On the Virtex 5 xcVLX330T FF1738 -2 board, this resulted in a 30% decrease in area.

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.