Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES) – An International Journal
ISSN: 2566-932X, Vol. 6, Issue 1, April 2022

Design and Implementation of High-Speed AES and Visual Cryptography with Modified Mix Column on FPGA – A Survey

Abibulla M
Department of ECE, AMC Engineering College, Bengaluru,India-560083, abibulla2000@gmail.com

Mohammed Shoaib Hafiz
Department of ECE, AMC Engineering College, Bengaluru,India-560083, mdshoaibhafiz@gmail.com

Isam Mansoor Khader
Department of ECE, AMC Engineering College, Bengaluru,India-560083, isam.khader@gmail.com

Chandra Babu D
Department of ECE, AMC Engineering College, Bengaluru, India-560083, dchandrababu2013@gmail.com

Abstract: Network security is one of prime importance with the advent of cyber-attacks, phishing and hacking occurring on a regular basis in the 21st Century. Though a lot of popular algorithms already exist for encrypting data such as AES, DES or Triple DES, there is a necessity for strengthening the existing algorithms to prevent a possible brute force attack on encrypted data. This paper explores a few papers aiming to achieve the same. It elaborates on the advantages and disadvantages of the existing algorithms and finally concludes with a proposal for a future implementation which can overcome the disadvantages.

Keywords: AES; Decryption; DES; Encryption; Triple DES; Visual Cryptography.

I. INTRODUCTION

Network or Data Security is an activity designed and controlled by a Network Administrator to guard the usability and integrity of your network and data. It involves both Hardware and Software technologies with an aim of targeting variety of threats. It stops them from entering or expanding on your network and typically manages access to the network. The security implementations in application domains cover both public and private computer networks that are utilized in everyday tasks for conducting communications and transactions among business partners, governed agencies and individuals. Cryptography is a programmed mathematical tool that plays a pivotal role in network security. It provides authentication to the users by assuring both, the sender and recipient the information with a proof, so later neither can deny having processed the information. Thereby, assuring the confidentiality and integrity of the data.

The cryptography approach consists of encryption and decryption algorithms. Encryption is a process which transforms the first information into an unrecognizable form. This newly formed message is on the whole different from the first one. Encryption is usually done using key algorithms. Decryption is a process of converting encoded/encrypted data into a form that is readable and understood by a person or a computer. This method is performed by un-encrypting the text manually or by using keys utilized to encrypt the first data. The reason for using Encryption and Decryption is that it helps to protect your confidential data such as passwords and login id, provides confidentiality of private information ensuring that the documents or file has not been altered. It's a crucial method because it helps you to securely protect data that you simply don't want anyone else to possess access. There are four sorts of keys used: Symmetric Key, Asymmetric Key, Public Key, Private Key & Pre-Shared Key. Symmetric-key encryption are algorithms which use an equivalent cryptographic key for both encryption of plaintext and decryption of ciphertext. In Asymmetric encryption, two pairs of keys are used. Public key cryptography is an encryption system which is predicated on two pairs of keys. Public keys are used for encrypting messages to a receiver. Private key could also be a part of a public/ private asymmetric key pair. It is often utilized in asymmetric encryption as you'll use an equivalent key to encrypt and decrypt data. In cryptography, a pre-shared key (PSK) may be a shared secret which was earlier shared between the 2 parties employing a secure channel before it's used.

The AES algorithm (also referred to as the Rijndael algorithm) is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts the plaintext to ciphertext using 128-, 192-, and 256-bits key length. Since the AES algorithm is viewed as secure, it's within the worldwide standard. The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to supply ciphertext. The number of rounds depends on the key size getting used. A 128-bit key size are so as of ten rounds, a 192-bit key size dictates 12 rounds, and a 258-bit key size has 14 rounds. Each of those rounds requires a round key, but since one key is inputted into the algorithm, this key must be further expanded to get keys for every round, including round 0.

Visual Cryptography which was developed by Moni Naor and Adi Shamir in 1994 is cryptographic algorithm to obscure image-based secret information which can be decrypted using Human visual system. The image to be encrypted is divided into n shares and transmitted. The divided share when obtained individual does not reveal any information of the image. The image could be decrypted only if the k out of the n shares is available by superimposing the obtained shares.

The field-programmable gate array (FPGA) is a set of electronic circuits (IC's) that consists of internal hardware blocks with user-programmable interconnects to customize operation for a selected application. The interconnects can readily be reprogrammed, allowing an FPGA to accommodate changes to a design or maybe support a replacement application during the lifetime of the part. Hardware implementation of AES on FGPA offers better resources efficiency, throughput and security compared to the software implementation.

II. LITERATURE SURVEY

Mohamed Nabil, Ashraf A. M. Khalaf, Sara M. Hassan [1] in their paper focused on the speed constraint during encryption process in AES. They proposed an algorithm which depends on pipelined processing method for reduction in processing time. The regular AES algorithm uses 26 clock cycles to encrypt the data but their pipelined approach reduces the number of clock cycles. In the traditional AES algorithm, the beginning of next block of encryption starts only after completing the present encryption process. This leads to usage of more clock cycles and more memory required to store the input bits for the next rounds. Whereas in their pipelined approach every new clock cycle will have a new encryption process started. The proposed algorithm has reduced the clock cycles to 12 as against 26 in case of traditional algorithm but ended up consuming more area than the later one.

T. Manoj Kumar, P. Karthigaikumar [2] proposed a new and an efficient key dependent AES algorithm which gives better avalanche effect on comparing with the existing AES algorithm. The key matrix in AES algorithm is used only in one transformation stage (add round section) and other stages become independent of the key making it easily revertible. To overcome this, they designed an algorithm where all operation performed using key. An XOR operation is performed on all the bytes in key and a parity bit is obtained which is used to determine the operations on each transformation on every round. After implementing in FPGA, the synthesis results showed that the Avalanche effect is slightly increased. The main setback of this algorithm is that is used twice the area occupied by the traditional AES algorithm.

S. Madhavapandian, P. MaruthuPandi [3] in their paper focused on lower area utilization and ONChip utilization of power. They researched in this article projecting an implementation by modifying Mix column in AES technique giving a compact structure with efficient Mix Column Boolean expression in the resource sharing architecture usage and gate replacement method. In Mix Column, Galois Field 2^8 is used in Substitution of data in AES flow. LUT utilization has redundant bits while implementing on FPGA as Efficient Mix Column Boolean Expression uses Resource sharing architecture and Gate replacement technique the overall utilization of redundant bit is reduced which reduces power consumption and cost of AES algorithm. They proposed an approach to reduce cost by removing redundant LUTs with the help of resource sharing technique. The main setback of this algorithm is its time complexity and to decrease it we need a modification in AES with an increased security.

[4] In this paper, Aaron Barrera, Chu-Wen Cheng, Dr. Sanjeev Kumar presented an improved mix column computation of AES. they focused on the development and analysis of an efficient AES-128 Mix Columns algorithm implementation in two different approaches. Their first approach involved building the circuit modules around the traditional row-column multiplication method which resulted in simple circuit configuration. Second approach focused on forcing a more parallel behavior into the circuit to align the input signals together potentially resulting in decreased delay. Results showed in their second approach using parallelism in signal processing results in less time delay, logic elements and virtual memory.

Shuang Chen,Wei Hu and Zhenhao Li in their paper [5] used deep pipeline and full expansion technology to implement the AES encryption algorithm on FPGA. They focused on eliminating the waiting time in the processing of the algorithm by using full pipeline technology to expand the processing of the entire algorithm into a one-way complete pipeline thus producing all the data for the next step. .Another approached which they have used is complete enroll where data is stored in distributed RAM which has less space but access to storage is parallel hence all the state data are stored in distributed RAM. In sub byte operation, there will be multiple s-box access operations but during the pipeline execution, which will result in s-box access congestion and hinder the operation of the pipeline. Therefore, they designed an s-box in Block RAM which has more storage space for each Sub Bytes operation of the state matrix, which allows the 16 bytes of the state matrix to perform Sub Bytes operations in parallel. They achieved a better throughput and speed but at the expense of increased storage which is their main drawback.

In [6] Santhosh Kumar R and co, explained Advanced Encryption Standard (AES) algorithm which can be implemented both by Hardware & Software. Compared to software implementation, hardware implementation gives better security & increased throughput. They showed for the increased performance Field-Programmable Gate Array (FPGA) is one of the prominent solutions. The paper showcases implementation result of entire AES algorithm. The mix column approach chosen by them is mathematically intense, as it need Galois Field multiplication to be carried out. But these multipliers

require consume more time and area when it comes to hardware implementation.

[7] In this paper, Authors S.Sridevi, Junas M, Sarah Jenifer, Lavanya focuses on reducing the area & delay in multiplication. AES encrypts 128 bits at a time & treats 128 bits as a grid of 4*4 matrix. Mix column transformation is linear operation in which the state array matrix is multiplied with constant square matrix. Mix column is performed by using mix column multiplier & addition of partial product is done using half adders. Mix column is implemented using the concept of Look Up Table (LUT), since 16 bytes (128 bits) is divided into 1 byte each byte of data is multiplied with 02 & 03 which involves 256 combinations. Hence when LUT is used area consumption is reduced.

[8] This paper by Rizky Riyaldhia, Rojalia, Aditya Kurniawanb focuses on reducing the time taken for encryption which increases as the number of data bytes increases. They proposed an algorithm with modified shift rows and S box for mix column transformation. Their experiment showed that every time the data bytes increases by 1024 bytes, then time computation increases by three milliseconds. The shift row transformation is modified by using array shift mapping and Mix column transformation is modified by using s box and eliminating the use of Sub byte transformation. The main drawback of this algorithm is that the modified sbox requires twice the area of the traditional Sbox. Result showed that the percentage improvement on encryption process is 86.143% and decryption process is 13.085%.

III. CONCLUSION

With the advent of digital technology and IOT the use of hand-held devices and other portable devices, there is a huge demand in enhancing security along with optimizing the area. Improvising the speed of execution of the AES algorithm can in turn lead to a minimal probability of cracking the same. With this, we design a high speed and area-efficient AES algorithm combined with Visual cryptography which involves various modifications in the input stage and Mix column multiplication. With the help of the proposed model of encryption, the data can be protected from hackers and the algorithm will be more suitable for low area implementation. This ensures the safety of data, thus encouraging the population of India to drift towards DIGITAL INDIA.

REFERENCES

[1] Mohamed Nabil, Ashraf A. M. Khalaf, Sara M. Hassan “Design and Implementation of Pipelined AES Encryption System using FPGA” International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-5, January 2020.

[2] Manoj Kumar, T., Karthigaikumar, P. A novel method of improvement in advanced encryption standard algorithm with dynamic shift rows, sub byte and mixcolumn operations for the secure communication. Int. j. inf. tecnol. 12, 825–830 (2020).

[3] S. Madhavapandian, P. MaruthuPandi, “FPGA implementation of highly scalable AES algorithm using modified mix column with gate replacement technique for security application in TCP/IP”, Microprocessors and Microsystems, Volume 73,2020.

[4] S A. Barrera, C. -W. Cheng and S. Kumar, "Improved Mix Column Computation of Cryptographic AES," 2019 2nd International Conference on Data Intelligence and Security (ICDIS), 2019.

[5] S. Chen, W. Hu and Z. Li, "High Performance Data Encryption with AES Implementation on FPGA," 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), 2019.

[6] Santhosh Kumar R, Shashidhar R, "Design of High-Speed AES System for Efficient Data Encryption and Decryption System using FPGA," 2018.

[7] S. Sridevi sathya priya, J. M., S. J. S. and L. A., "Implementation of Efficient Mix Column Transformation for AES encryption," 2018 4th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, 2018.

[8] Rizky Riyaldhi, Rojali, Aditya Kurniawan, ”Improvement of Advanced Encryption Standard Algorithm with Shift Row and S.Box Modification Mapping in Mix Column”, Procedia Computer Science, Volume116,2017.