Design of Cryptographic Encryption Processor

Abhishek Kunte[1] and Dhanabal R[2]
[1]MTech. VLSI Design, Department of Micro & Nanoelectronics, Vellore Institute of Technology, Vellore, India
[2]Associate Professor, Department of Micro & Nanoelectronics, Vellore Institute of Technology, Vellore, India

Abstract

Cryptography still serves to be a major way for communicating highly confidential information. Hence it is essential for a cryptographic processor to have high performance, low power, flexibility in hardware and most importantly highly encrypted data set which could not be hacked by any other unauthorized person. While there are various algorithms available for cryptography, all algorithms focus on encrypting the data in different ways such that the data remains private and can be accessed via highly confidential private key.

In this work, the data is encrypted using modified AES algorithm by passing it through various stages of LUT's and shift registers. The multiple stages of encryption ensure highly encrypted data set. The performance metrics of the processor is measured on various parameters like throughput, power consumed, etc.

By using the modified AES algorithm for encryption, the processor achieves a throughput of 4Gbps for one program element block at 1GHz frequency.

Keywords

AES algorithm, Cryptography, LUT's, Shift Registers, Throughput.

I. INTRODUCTION

Cryptography is defined as the science of converting message into an unrecognizable form using a secret code called key to make it protected and resistant to stealing of information. Cryptography is one of the mostwell-known data security algorithms and has been used since it was introduced in 1976 and is used till date [1].

Secure information transfer is a vital part in communication. Making random changes in secret keys raises the provision of security and complexity of the cryptography algorithms.However, the algorithms consume memory spaces and execution time. In Nov 2001 NIST selected Advanced Encryption Standards (AES) [1] [2] for secure communication.

In AES algorithm, the same binary key is used for encryption and decryption purpose. Hence, AES algorithm is also called as symmetric key cipher.In cryptography, the encryption operation converts the normal data blocks known as 'plain text' into an encrypted text known as the 'cipher text' with the help of a 'key'. The decryption converts back this 'cipher text' to the original 'plain text' using the same 'key'. This paper proposes a modified AES algorithm. The proposed modification in the Program Element block can improve the throughput and performance of the functional units with the help of Instruction Level Parallelism (ILP) [3]. Results show that the area efficiency and the throughputof the processor using modified AES algorithm is better over the other processors in literatures [4].

II. OVERVIEW OF THE AES ALGORITHM

The Advanced Encryption Standard (AES) is a symmetric cipher which is used in cryptography. Using AES, the data is processed and encrypted in 128-bit blocks. AES mandates the block size of 128 bits and the choice of key size from 128bits, 192bits, and 256 bits with these variants which are referred to as AES128, AES-192, and AES-256, respectively. Depending on the specified key size, AES implementations use 10,12 or 14 rounds. The block state in AES is organized in a 4x4 block and is maintained as an array of 16 bytes. Initially, the state is filled from the input blockcolumn by column. The stateis transformed in N_r rounds to a final state as the output block, which is then read out through successive columns. For encryption, all is comprised by an identical sequence of operations on the current block state except the final round. The final round differs such that it excludes the mix column operation [5].

Following is the basic structure of AES:

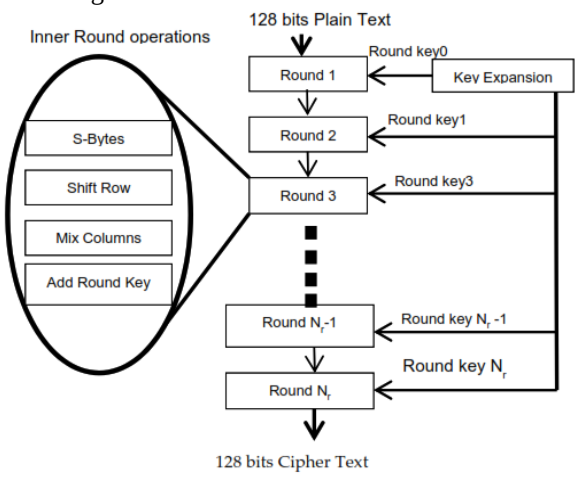

Fig.1: Flow of AES Encryption algorithm

III. EXISTING ARCHITECTURE OF CRYPTOGRAPHIC ENCRYPTION PROCESSOR

It can be seen from Fig.2. that architecture consists of anExecution Tile as the functional part.It has State Engine (SE) as thefront-end along with a 256-entry register file.

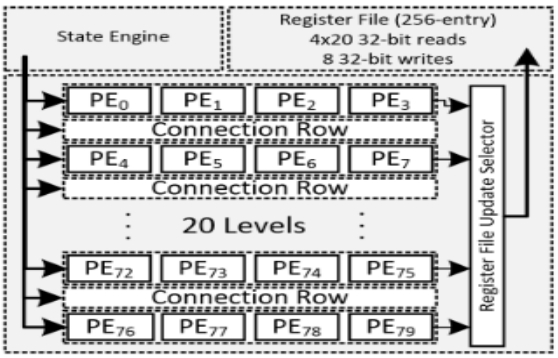

Fig.2: Architecture of Cryptographic Encryption Processor

The front-end block shown in Fig.2. is controlled by a hardwarestate machine.This is configured as part of the initial setup. The configuration remains fixed as long as there is no change in the algorithm. The state counter and a small control memoryblock are the part of SE.The Execution Tile encapsulates all functional partsof the architecture. It consists of multiple identical stages.Each of these stages has a number of Processing Elements (PEs) connectedto the next stage by Connection Row (CR). It can be seen from the Fig.2 that, the Execution tile contains of a number of PEs and CRs, and loopbackconnections from each stage to a register file [6].

IV. ENCRYPTION USING MODIFIED AES ALGORITHM

The PE block shown in Fig.2. operates on modified AES algorithm.

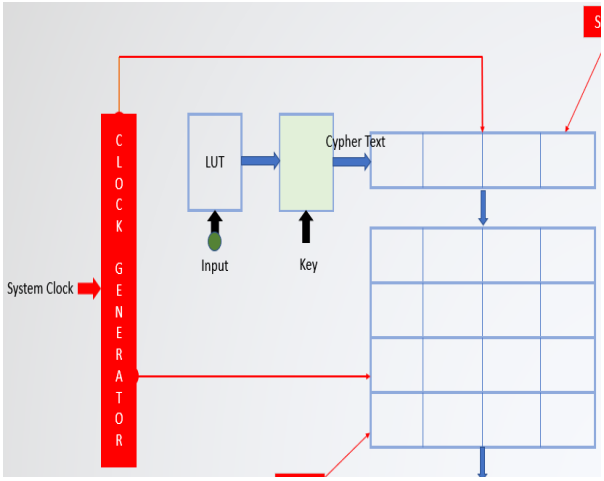

Fig.3: Flow of the modified AES algorithm

In this proposed AES algorithm, the data is encrypted in two stages namely:

1) Using Look Up Table (LUT).

2) Using Matrix Column Transformations.

The LUT is purely made up of combinational logics where the 8-bit input data is XORed as shown in Fig.4(a).

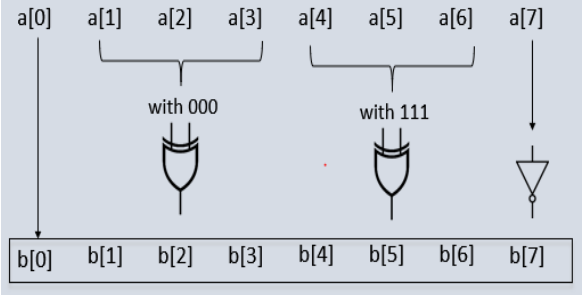

Fig.4(a): Data encryption using LUT

The 8-bit output obtained from this stage is then XORed with the 8-bit private key to form a ciphertext.

The ciphertext is then passed through a Serial Input Parallel Output (SIPO) register which takes these 8-bit ciphertexts in a group of four and converts into 32-bit data stream.

The system operates using the concept of pipelining. Pipelining is basically a technique where the second instruction begins executing before the first one has been completed. The pipeline is divided into various segments of reasonably equal complexity.Eachof these segmentsperforms its operation in tandem with the other segments. When a segment completes its operation, it passes the result to the next segment in the pipeline.This technique effectively increases the computational speed and hence is used in most of the advanced processors.

The processor uses two level pipelined architecture.While the 32-bit data is being passed in the Matrix, next data is also processed in tandem in the LUT stage.

The encrypted data from the LUT is again processed in the group of 4 in Matrix form as shown in Fig.4(b).

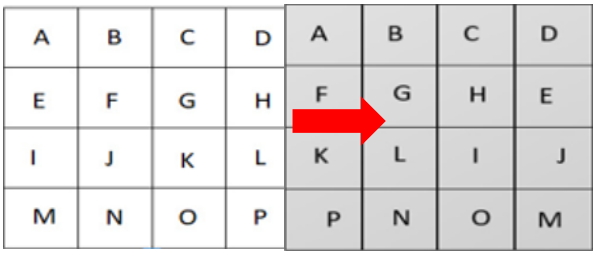

Fig.4(b): Data Encryption using matrix column transformations

This two-stage encryption ensures more security than the classical AES algorithm.

The pipelining also ensures that the overall throughput of the system remains high.

V. DECRYPTION

The decryption can be done in the exact reverse order. However, the private key should be available in order to decrypt the data. If the processor is made reconfigurable, then it can be used either for encryption or decryption at any time. Another way of doing this is using scripting language wherein the encrypted data stream is taken along with the private key; stored in the form of arrays and operated upon in the exact reverse order to get back the original plain text. But this has some serious drawbacks and is not recommended as the pattern can be tracked and chances of data hacking are more. So, the ASIC implementation of the decryption processor is suggested.

VI. RESULTS

While the program element using conventional AES algorithm gave throughput of 1.6Gbps; from the simulation results it is found that the throughput obtained for one program element using the modified AES algorithm is 4Gbps. Hence, if we use 80 such program elements in the existing architecture of the cryptographic encryption processor, overall throughput of about 320Gbps can be achieved. Pipelined architecture of the processor gives high throughput. The modified AES algorithm gives a very highly encrypted data set than the classical AES algorithm due to two step encryption process. Thus, using modified AES algorithm has not only increased the encryption standards but also has given an increase in throughput.

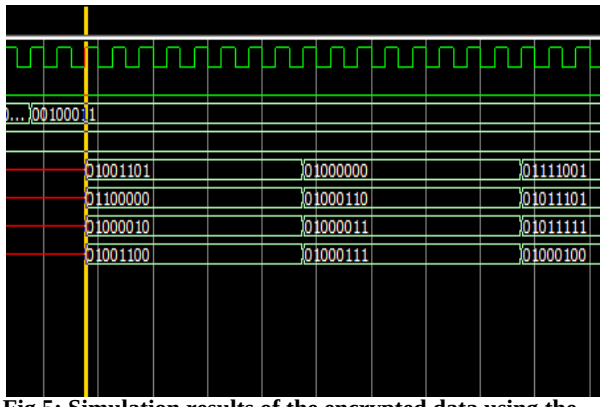

Fig.5: Simulation results of the encrypted data using the modified AES algorithm

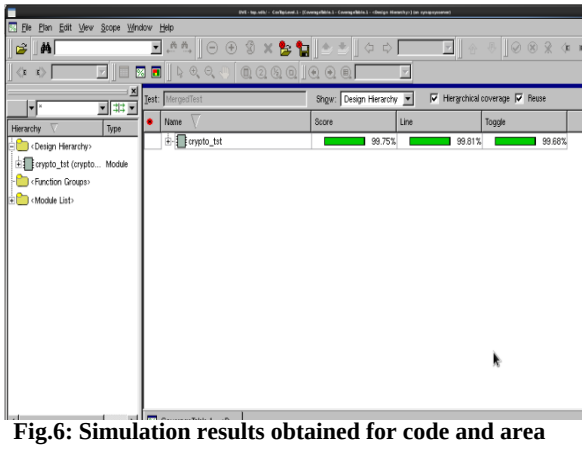

Fig.6: Simulation results obtained for code and area coverage

VIII. CONCLUSION

The cryptographic encryption processor is hence designed and implemented using modified AES algorithm. The performance of the processor is tested and based on the simulation results it is found that it gives the throughput of about 4Gbps for one programming block for an operating frequency of 1GHz. This increased in throughput though comes at an additional overhead of pipelined blocks. The modified AES algorithm thus increases throughput significantly (by around 150%) along with providing highly encrypted data set.

REFERENCES

[1] Amit Kumar, Manoj Kumar, and P. Balramudu"Implementation of AES algorithm using VHDL", Proceedings of the IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC).

[2] Ukrit Arom-oon "An AES Cryptosystem For Small Scale Network", Third Asian Conference on Defence Technology (3rd ACDT).

[3] Shoucheng Wang, Jinhui Xu, Yingjian Yan and Gongli Li, "A High-Efficiency Reconfigurable Cryptographic Processor", 2016 IEEE International Conference on Integrated Circuits and Microsystems.

[4] Ross Anderson, Mike Bond, Jolyon Clulow andSergei Skorobogatov"Cryptpgraphic Processors – A Survey".

[5] Amar Rasheed, M. Cotter, B. Smith, D. Levan, and S. Phoha "Dynamically Reconfigurable AES Cryptographic Core for Small, Power Limited Mobile Sensors", 978-1-5090-5252-3/16/$31.00 ©2016 IEEE.

[6] Gokhan Sayilar and Derek Chiou "Cryptoraptor: High Throughput Reconfigurable Cryptographic Processor", 978-1-4799-6278-5/14/$31.00 ©2014 IEEE.