STUDY OF DIFFERENT FPGA SYSTEMS IMPLEMENTED AES ALGORITHM: A REVIEW

1Sharayu Sharad Karwade, 2Dr. Kalyani Akant
1PG Scholar, 2Associate Professor
1-2Department of Electronics & Telecommunication Engineering,
1-2G H Raisoni College of Engineering, Nagpur, Maharashtra, India.

Abstract: With the rapid growth of multimedia technologies, cryptography is considered as one of the most secured ways for transmitting and receiving data. Now a days AES algorithm is not only limited to transmit video data but also for image and text transmission. In this paper we have reviewed four FPGA boards on which AES algorithm has been implemented.

Keywords-FPGA, AES, Xilinx, DSP.

I. INTRODUCTION

Cryptography is the technique of preserving data from unwanted objects by transforming the pattern that is unrecognizable by hackers while transmission. Encryption is the process where maximum part of information is scrambled like text-data, images, audio, and video so that the data undecipherable, unseen until the process is done. The primary objective of cryptography is to protect information from non-authorized hackers. The data decryption/decryption is nothing but the receiving of encrypted data which recreates the original information. At present cryptography is not limited to secure military data but known as one important method for policy of security considering any organization and recognized as standard for industry for giving secure data, access control, and financial agreement through electronic medium. The primary information that will be send or saved is known as plaintext, which either a person or machine can read. Whereas the hidden information called cipher text, which is not readable, neither by a person nor by any device can accurately processed until it is decrypted. The implementation is done by either software or hardware. For analyzing cryptography algorithms on hardware the most efficient solution is provided by Field Programmable Gate Arrays (FPGAs) [18]. Xilinx ISE suit provides easy medium between software and hardware. There are different kits for performing operations through FPGA. FPGA is the most advance platform for performing various applications. This paper describes different FPGA boards on which the AES algorithm has been performed successfully.

In section II the cryptography procedure and brief information about AES algorithm is described. Section III is describes about FPGA working and how AES algorithm is used on FPGA. In section IV different FPGA systems and results on that particular kit are described. Conclusion is given in section V.

II. CRYPTOGRAPHY

Cryptography is the technique of preserving data from unwanted objects by transforming the pattern that is unrecognizable by hackers while transmission. Encryption is the process where maximum part of information is scrambled like text-data, images, audio, and video so that the data undecipherable, unseen until the process is done. The primary objective of cryptography is to protect information from non-authorized hackers. The data decryption/decryption is nothing but the receiving of encrypted data which recreates the original information. At present cryptography is not limited to secure military data but known as one important method for policy of security considering any organization and recognized as standard for industry for giving secure data, access control, and financial agreement through electronic medium. The primary information that will be send or saved is known as plaintext, which either a person or machine can read. Whereas the hidden information called cipher text, which is not readable, neither by a person nor by any device can accurately processed until it is decrypted. The implementation is done by either software or hardware. For analyzing cryptography algorithms on hardware the most efficient solution is provided by Field Programmable Gate Arrays (FPGAs) [18]. Xilinx ISE suit provides easy medium between software and hardware. There are different kits for performing operations through FPGA. FPGA is the most advance platform for performing various applications. This paper describes different FPGA boards on which the AES algorithm has been performed successfully.

In section II the cryptography procedure and brief information about AES algorithm is described. Section III is describes about FPGA working and how AES algorithm is used on FPGA. In section IV different FPGA systems and results on that particular kit are described. Conclusion is given in section V.

2.1 Advance Encryption Standard (AES)

In 1997, the national bureau of standards asked for a fresh standard which will replace the data encryption standard. The contest ends in November 2001 as they chose the Rijndael crypto-system as the Advanced Encryption Standard (AES) [3][7]. The Rijndael system operates on blocks of 128 bits, every 8 bit inputs arrange as 4 × 4 matrices. The technique uses variable block length and a key length, any combination of keys lengths is allowed latest specification.
Figure 1: The AES encryption and decryption flow [5]

Other than 128 bits key length AES also uses 192 and 256 bits of key size blocks called AES-192 and AES-256 respectively. The AES-128 uses 10 rounds, AES-192 uses 12 rounds and AES-256 uses 14 rounds.

III. FPGA

It is a semiconductor device having programmable logic blocks and interconnection system. At its core, FPGA is an array of interconnected digital sub circuits that performed regular functions while also offering very high levels of flexibility. Even after the product released in the market FPGA can implement any logical function as an ASIC can and we can re-program it [5].

Figure 2: Internal structure of FPGA [6]

3.1 Implementation of AES algorithm in FPGA

In FPGA 128 bits key length AES algorithm is used. As Aes-128 has 10 rounds and divided into 4 stages. These stages are as follows:

1) Subbyte transformation: In this it splits the subbytes into phases and then pass each one through a box called substitution box. Substitution information is provided from look up table [7].

2) Shiftrow transformation: In this the rows of the state array are shifted cyclically to generate diffusion.

3) Column-Mix Transformation: Columns are operated individually; it mixes every four byte of each column to form a new value. According to Galois Field (GF) rule the operation is performed dot wise [8].

4) Add-round Transformation: The Ex-ORing is performed around round key and state having each key length sized 128 bits. This is a column wise operation takes one word from round key and state columns four bytes.

There are different ways to implement this algorithm in field programming gate array some of the FPGA systems on which AES algorithm are being performed are described as follow.
IV. FPGA SYSTEMS

4.1 SPARTAN 3 FPGA

Fig. 3: Spartan-3 family architecture [9]

Figure 3 shows the spartan-3 family architecture which contain configurable logic blocks and block RAM for implementation of logic and storing purposes that can be use as flip-flop or latches. Block RAM can provide the storage up to 18KB dual port block. It has up to 633 I/O pins. Two 18bit binary numbers is accepted as input and calculate the result by multiplier. Digital clock manager (DCM) blocks give entire digital solutions for distribution, delay, multiplication, division, and phase shifted clock signals [9].

4.2 Implemented Results

Fig. 4: Proposed block diagram for AES algorithm using spartan-3[10]

In above configuration spartan 3 EDK, device-XC3S200, package-TQG144, speed grade of -4 is been used. The advance AES algorithm is implemented. On the opposite hand, synthesis results show that area consumption is low, using simply 100 percent of logic circuits of FPGA for AES, allowing the implementation of this method over affordable FPGA’s [10].
4.3 Virtex 5 FPGA

Figure 5 shows Slice element structure in Virtex-5. It utilized the second generation Advanced Silicon Modular Block (ASMB) column wise family of vertex 5 includes five different sub systems, the maximum assortments provides by no other FPGA system. It has most developed high performable fabriccable logic. Virtex 5 FPGA has various system level blocks of hard IP, 36-Kbit block RAM/FIFOs are also included, 25 x 18 DSP slices of second generation, built-in digitally-controlled impedance is with SelectIO technology, interface blocks of chip sync sourcesynchronous, functionality system monitor, advance tiles clock management with integrated managers with digital clock and phase locked loop, and latest configurating choices [12].

4.4 Implemented Results

In the above module the pielined structure of AES algorithm and parallel processing has been focused. Virtex-5FPGA board had been used with software Xilinx ISE 8.1i. New methods for performing AES operations at high throughput using on chip BRAM and DSP blocks with comparatively less use of traditional user logic such as flipflops, look up charts is been presented. This perticuler design methodology is to be supported by encryption and decryption standard [13].
4.5 Altera Cyclone-II FPGA

![Cyclone-II block diagram](image)

Above figure shows the block diagram of cyclone II. Cyclone is a low cost production of Altera Corporation. It is a two-dimensional row and column based architecture. It consists of 16 logic elements in each logic array block. M4K memory block has 4K bits of memory. Multiplier can be implemented up to two 9x9 bit multiplier. It has four PLL devices.

4.6 Implemented Results

![Structure for AES encryption and decryption systems](image)

Entire structure shown in above designed decreases AES encryption and decryption system which is shown in Fig. 2, encryption unit is the upper half part, the second part is decryption unit [14]. In this FPGA Altera Cyclone EP2C35F672C6 is been used and tested for AES algorithm, it provides less hardware compare to pipeline AES algorithm. Throughputs for encryption and decryption within total 760 logic elements are 593.45Mbps 267.63Mbps respectively. These results make this system more secure, dependable and cost efficient.
4.7 Atrix 7 FPGA

Artix 7 FPGAs are optimized for the lowest in prize and power with large volume automotive applications and small form factor packaging [17]. It has 36 Kb dual-ports block RAM accompanied by built-in FIFO logic for on-chip data buffer. It has also advance speed of serial connectivity added with in-build serial transceivers starts from 500 Mb/s upto 6.25 GB/s of maximum rates. It has large variety of configuration options; with HMAC/SHA-256 authentication it supports upto 256-bit AES encryption.

4.8 Implemented Results

AES 128 bit key algorithm implemented on artix 7 Nexys 4 kit proposed a platform using AES algorithm for encryption and decryption without having a personal computer. Including feedback loops all the complexities of the algorithm is being handled by artix 7 systems efficiently [18]. This result provides the encryption by using 128 bits key on Artix 7 FPGA board successfully which can be expanding for further use of 192 bits & 256 bits key [18].

V. CONCLUSION

In this paper, we have surveyed the AES algorithm implemented FPGA systems. We have given brief information about different FPGA kits and then implemented results have been provided. The analysis gave us interesting results about how the advancement in FPGA systems is done. What changes have been done in AES algorithm according to application has been described in this paper. We can conclude that FPGA is a good platform for implementing AES algorithm. There are various ways to use AES algorithm and FPGA boards depending upon the application.

REFERENCES


Fig. 9: Block Diagram of Artix-7 FPGA [16]


[15] Yang Jun, Ding Jun, Li Na, Guo Yixiong “FPGA-based design and implementation of reduced AES algorithm”, 2010 International Conference on Challenges in Environmental Science and Computer Engineering. DOI:10.1109/CECSE.2010.123

