NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 3, ISSUE 1, JAN.-2016

ADVANCED ENCRYPTION STANDARD WITH LOW AREA & POWER ON FPGA MODULE

Assi. Prof. Sarika N. Wagaj
Department of Electronics and Telecommunication, VVPIET Maharashtra India

Assi. Prof. Preeti Kadam
Department of Electronics and Telecommunication, VVPIET Maharashtra India

Assoc. Prof Sajid Shaikh
HOD, Department of Electrical & Electronics, VVPIET Maharashtra India

ABSTRACT

Security of the data is most important aspect in communication. In global world security of data is very common parameter. There is need for secure transaction in networking, communication, commerce, and secure messaging has moved encryption into the commercial area. Advanced encryption standard (AES) was issued as Federal Information Processing Standards (FIPS) by National Institute of Standards and Technology (NIST) as a successor to data encryption standard (DES) algorithms. The high level of security and the fast hardware and software implementations of the Advanced Encryption Standard (AES) have made it the first choice for many critical applications. For secure data transmissions in wireless military communication and mobile telephony requires encryption with limited area constraints. Therefore, the current work will be focuses on designing and simulating low area AES encryption module and calculate power.

Advanced Encryption Standard is a symmetric key block cipher encryption algorithm. Understanding the need proposed work introduces the design and simulation of the block cipher 128 bit Advanced Encryption Standard (AES-128) with low area constraint. I propose low area design by reduction of area occupancy which will be offered.

Keyword: Advanced Encryption Standard (AES), Rijindael Cipher Key (128 bit), and Field Programmable Gate array (FPGA), Data Security.

INTRODUCTION

The design consists of AES algorithm design which is a symmetric encryption algorithm processing data in block of 128 bits. A bit can take the values zero and one, in effect a binary digit with two possible values as opposed to decimal digits, which can take one of 10 values. Under the influence of a key, a 128-bit block is encrypted by transforming it in a unique way into a new block of the same size. AES is symmetric since the same key is used for encryption and the reverse transformation, decryption. The only secret necessary to keep for

security is the key. AES may configure to use different key-lengths, the standard defines lengths. Each additional bit in the key effectively doubles the strength of the algorithm, when defined as the time necessary for an attacker to stage a brute force attack, i.e. an exhaustive search of all possible key combinations in order to find the right one Bytes .The basic unit for processing in the AES algorithm is a byte, a sequence of eight bits treated as a single entity.
AES performs bulk encryption of information as ECB (extended code block) code type.AES is a symmetric algorithm which process 128bit stream in 10 rounds. It uses 4 stage structures in single round to form a cipher text for respective round. The basic unit of AES algorithm process is a byte and this algorithm is based on Substitution Permutation network it means it has series of linked mathematical operations. AES consist of two dimensional array called as state. The AES algorithm is basically used in transfer mode machines for security of transactions. AES mainly implemented in many platforms of languages i.e. Matlab, C and Java, but as for reconfiguration purpose we propose to design of AES in VHDL language. The AES algorithm is used in broad applications, including smart cards and cellular phones, WWW servers and automated teller machines (ATMs), and digital video recorders. As compared to Software implementations, hardware implementations of the AES algorithm provide more physical security as well as higher speed. VHDL is used in order to design the hardware elements, which will be run-time reconfigured. Some important features of VHDL are: it is one of the most used HDL, it has a large and flexible syntax which allows to describe a circuit by using different abstraction levels (structural, data flow, or hardware behavior), it is possible to indicate low- level constraints (like place-and-route constraints), etc. All these features have motivated us to use VHDL.

VHDL uses component level synthesis when the first phase finishes with the first block to be encrypted; this next block goes into that phase while the first block goes into the next operation. Finally, we have used parallelism of code for calculating total cipher text or original plain text. VHDL language supports most widely used reconfigurable electronic hardware platform which is FPGA (Field Programmable Gate Array).FPGA basically consist of CLBs (Configurable Logic Blocks) which is mainly used for optimization with minimum use of no of logical block and slices. FPGA device directly provides routing and switching between different I/Os. It simulates and creates RTL schematic of design along with VHDL language. The basic operation of a symmetric key block cipher with 128 bit blocks and a 128 bit key is shown in Figure2.1A block cipher operates on fixed-length blocks of data, while symmetric key algorithms use the same key for encryption and decryption. Using the all parameter we have to design the encryption as well as decryption system. Symmetric data can be cipher using the cipher key, same cipher key is used for encryption as well as decryption of data.

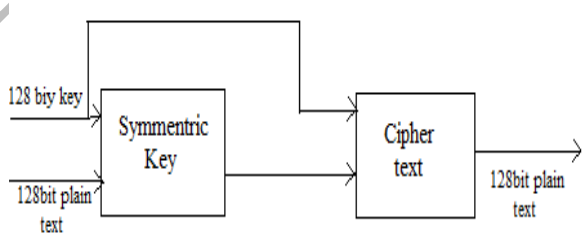

Fig.1: Basic AES system

Fig 1 shows the standard AES algorithm operates on 128 bit blocks of data at a time, which is twice the block size of DES. AES supports keys of 128, 192, or 256 bit keys. The first stage of the algorithm is the Key Expansion function which uses the Rijndael key schedule to produce separate 4x4 matrix of keys for each of the 10 encryption rounds used. Each round of encryption operates on a 4x4 matrix of bytes called the state and each encryption round has four stages or transformations: Sub Bytes, Mix Columns, Shift Rows, and Add Round Key.

LITERATURE REVIEW

Mobile workers known in some circles as road warriors increasingly are becoming important players in today's fast-paced world of business. They are the people who are always on the go the ones who spend at least half of their workweeks away from their regular offices. Thus, they have to use laptop computers, personal digital assistants (PDAs), and portable memory devices to exchange and transport business-critical data. [9] In many cases, the security of this data hinges on the physical safety of the devices. A 2006 global study by market research firm Gartner indicates that while 25 % of information theft is linked to network intrusion, 60 % of data breaches can be attributed to lost or stolen mobile devices. With this in mind, it is critical for organizations to bolster defenses by encrypting data across the board.

Data Security: Enterprise businesses and government agencies around the world face the certainty of losing sensitive data from a lost laptop, removable media or other plug-and-play storage device. This drives the need for a complete data protection solution that secures data on all common platforms, deploys easily, scales to any size organization and meets strict compliance requirements related to privacy laws and regulations. [9]Benefits of encryption: Encrypting data on mobile devices eliminates the dangers associated with loss or theft. The process makes data worthless to unauthorized users. Typically, by processing data through a mathematical formula called an algorithm, encryption software converts data into "cipher text." Following this conversion, that data requires users to input their unique credentials to gain access to it. Provided those credentials stay private, they make it virtually impossible for others to access the data. [5]

Data Encryption Standard (DES) was one such encryption algorithm. The DES expired in 1998 and the US National Institute of Standards and Technology (NIST) announced an open international competition for cipher designs to replace DES as the federal information processing standard. [1]Rijndael won the competition based on security, simplicity, and suitability for both hardware and software implementations, and was designated the Advanced Encryption Standard. AES, like DES, is a symmetric key block cipher encryption algorithm.

Announcing the Advanced Encryption Standard (AES) is by Federal Information Processing Standards Publication 197, November 26, 2001. The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm has asymmetric block cipher that can encrypt (encipher) and decrypt (decipher) the information. Encryption converts data to an unintelligible form called cipher text, decrypting the cipher text converts the data back into its original form, called plaintext. This standard specifies the Rijndael algorithm that is AES algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.

"An Efficient VLSI Implementation of AES Encryption Using Rom sub modules and Exclusion of Shift rows" has Seena.S.Das Dept.of Electronics & Communication LBS". The

constraints of area and power are the challenges for the cryptographic algorithms to be implemented. [2] In this paper, the implementation of Advanced Encryption Standard (AES) encryption algorithm is proposed in terms of resource and power optimization.

"Area and Power optimization for AES encryption module implementation on FPGA" has Tuan Anh Pham, Mohammad S. Hasan and Hongnian Yu Faculty of Computing, Engineering and Technology Staffordshire University Stafford, UK; International Conference on Microelectronics, 2014. The design is based on [4] optimized area by using the time sharing of certain resources and iteration architecture. In this research work the design is developed by using design optimized logic circuit, timing control blocks, and state machine.

"Design and implementation of area optimized AES algorithm on reconfigurable FPGA" paper at International journal of Computer Science and its Applications by M.SirinKumari , D.Mahesh Kumar Y. Assoc.Prof, Rama Devi at JITS Kanpur. This paper [6] addresses design, hardware implementation and performance testing of AES algorithm. An optimized code for the Rijndael algorithm with 128-bit keys has been developed.

METHODOLOGY

The AES algorithm has 4 phases that execute the process in sequential manner. The encryption process is achieved by processing plain text and key for initial and 9 rounds, Same decryption is takes place but in reverse manner. A 4x4 state is formed in each round and particular length data is introduced in it for encryption process. The 10, 12, 14 rounds are there for 128, 192,256 bits in length respectively. Initially a key expansion process is used to expand the basic 16 byte key into 11 arrays of total 44 words. Due to this the 16 byte key is converted into 176 byte i.e. 44words which are further used for 11 rounds. AES is basically a recent cryptographic security algorithm, and in our proposed structure we uses basically symmetrical structure of 128 bit i.e. 11 round process.

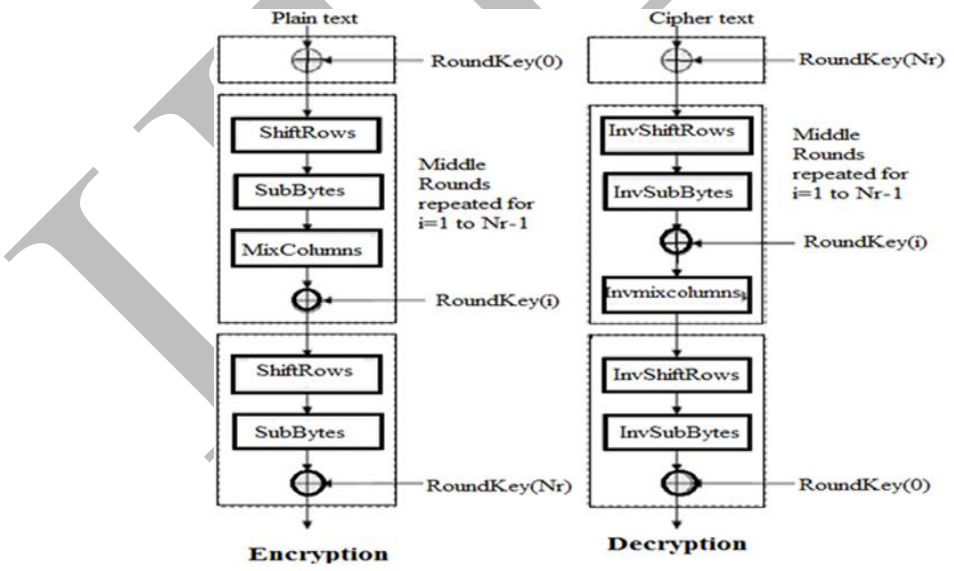

Fig.2: AES Encryption and Decryption data flow.

Out of these 11 rounds 1 round is used for initialization purpose and remaining 10 are used for AES actual process. There are mainly two logical steps for key expansion based on either the key is multiple of 4 or it is not multiple of 4. Once the key is expanded same key is used for encryption and decryption process to achieve symmetric AES structure. Fig.2 the each round consists of total 4 phases used for formation of cipher text as a output of the respective step and that output feuded as input for next successive round. The overall process is same for next 10 round till formation of cipher text is completed ,but for all these rounds keys are differ that are derived from words (as output of key expansion unit)from w0 to w43.

SUB BYTE PHASE: -- This Sub Byte transformation is a non-linear byte substitution which operates independently on each byte of the State using the S-box table. S-box table contains 256 numbers (from 0 to 255).

SHIFT ROW PHASE:--In the Shift Row transformation, the bytes in the last three rows of the State are cyclically shifted over1,2 and 3bytes respectively. In Shift Rows transformation, the rows of the state are cyclically left shifted over different offsets. Row 0 is not shifted; row 1 is shifted one byte to the left; row 2 is shifted two bytes to the left and row 3 is shifted three bytes to the left.

MIX COLUMNS PHASE:-The Mix Columns transformation operates on the State column by column, treating each column as a four-term polynomial.

ADD ROUND KEY PHASE:-The Add Round Key phase performs an operation on the State with one of the sub keys. The operation is a simple XOR between each byte of the State and each byte of the sub-key. As initially 11 arrays are formed out of that 1 use for initialization process and from that array key expansion is done. Thus the keys formed total W43 which are used further for next 10 rounds. Each round uses 4 word key along with plaintext/cipher text.

CONCLUSION

This paper has two primary goals, the first of which is to improve performance of the baseline design of AES targeting an 8-bit platform based on the chosen metrics. The second goal of this research is to quantify how each factor interacts and affects the overall values of each metric and to identify which factors are responsible for the largest variance in performance of the AES algorithm measured in throughput, area efficiency, and area occupied.

This synopsis presents an overview of the proposed system which is "Area and Power Optimization for AES Encryption Module on FPGA. The optimization achieved by minimizing number of slices to reduce number of logical blocks and memory requirements. The proposed architecture provides simplest and optimized area and power.

REFERENCES

[1] *"Novel Architecture for Inverse Mix Columns for AES using Ancient Vedic Mathematics on FPGA"* Sushma R Huddar, Sudhir Rao Rupanagudi, Dept. of FPGA & VLSI World Serve Education, Bangalore, India {sushma, sudhir}@worldserve.in.

[2] *"An Efficient VLSI Implementation of AES Encryption Using Rom sub modules and Exclusion of Shift rows"* Seena.S.Das Dept. of Electronics & Communication LBS Institute of Technology for Women Thiruvananthapuram,India,Seena.234@gmail.com.in December 2014.

[3] *"Efficient Implimentation of AES Algorithm on FPGA"* Hrushikesh S. Deshpande, Kailash J. Karande, AltaafO. Mulani April 2014.

[4] *"Area and Power optimization for AES encryption module implementation on FPGA"* Tuan Anh Pham, Mohammad S. Hasan and Hongnian Yu Faculty of Computing, Engineering and Technology Staffordshire University Stafford, UK, tapham@live.com

[5] "Understanding *AES Mix-Columns Transformation Calculation"* Kit Choy Xintong University of Wollongong, Year 3, Student kit_4ever2003@yahoo.com

[6] *"Design and Implementation of Low-are and Low-power AES Encryption Hardware Core"* Panu Hämäläinen, TimoAlho, Marko Hännikäinen, and Timo D. Hämäläine Tampere University of Technolog / Institute ofDigital and Computer Systems P. O. Box 553,FI-33101,Tampere, Finland{panu.hamalainen timo.a.alho,marko.hannikainen, timo.d.hamalainen}@tut.fi

[7] *"High Throughput – less Area Efficient FPGA Implementation of block cipher AES Algorithm"* M.SIRIN KumariD. Mahesh Kumar Y.Rama Devi(M.TECH) II year Assoc.Prof M.TECH(DC). JITS-KNE

[8] *"FPGA Implementation of Efficient Hardware for the Advanced Encryptio Standard"* International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-3, February 2013 By Amandeep Kaur, Puneet Bhardwaj, Naveen Kumar

[9] *"Cryptography and Network Security"* By William Stallings.