International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

HIGH SPEED OPTIMIZED AES USING PARALLEL PROCESSING IMPLEMENTATION

R.Jerlin Emiliya[1], D.Delphy[2], B.Sangeetha[3]

[1]*Associate professor hod of ece*
[2]*Assitant professor*
[3]*PG student, Dept. of ece, As Salam college of engg & tech, Tamil Nadu India*

Abstract - *Advanced encryption standard (AES) algorithm has been widely deployed in cryptographic applications. This work proposes a low power and high throughput implementation of AES algorithm using key expansion approach. We minimize the power consumption and critical path delay using the proposed high performance architecture. It supports both encryption and decryption using 256-bitkeys with a throughput of 0.06 Gbps. The VHDL language is utilized for simulating the design and an FPGA chip has been used for the hardware implementations. Experimental results reveal that the proposed AES architectures offer superior performance than the existing VLSI architectures in terms of power, throughput and critical path delay.*

Key words: *AES, VHDL, FPGA, Encryption, Decryption.*

1. INTRODUCTION

The recent years, there is a growing requirement to implement cryptographic algorithms in fast rising high-speed network applications. Encryption is the process of encoding information so that the unauthorized persons cannot identify the information. All the encryption algorithms convert the available information into unreadable secured form, referred to as cipher text. The authorized person will be able to decode the information using decryption algorithms. Two types of cryptographic systems available for data security are asymmetric (public-key) and symmetric (secret-keycryptographies (Hosseinkhani and Javadi, 2012). Asymmetric cryptography utilizes separate keys for encryption and encryption process for the key transportation mechanism. Conversely, symmetric cryptography utilizes an identical key for both encryption and decryption process, which is effective while handling a large amount of data (Chen et al.,2011).

2. LITERATURE SURVEY

J. Daemen and V. Rijmen et al [1] Rijndael Algorithm is the importance of cryptography applied to security in electronic data transactions has acquired an essential relevance during the last few years. A VHDL- based implementation of the Advanced Encryption Standard (AES) algorithm is presented in this paper. The design has been coded by Very high speed integrated circuit Hardware Descriptive Language. All the results are synthesized using Xilinx ISE and simulated by using ModelSim software.

Peter J. Ashenden et al [2] "The Designer's Guide to VHDL", Advanced Encryption Standard can be programmed in software or built with pure hardware. This implementation is compared with other works to show the efficiency. All the transformations of both Encryptions and Decryption are simulated using an iterative design approach in order to minimize the hardware consumption. This research investigates the AES algorithm with regard to FPGA and the Very High Speed Integrated Circuit Hardware Description language (VHDL). Simulation results, performance results are presented and compared with previous reported designs.

3. ENCRYPTION

The Encryption process of Advanced Encryption Standard algorithm is presented below, in figure 1. This block diagram is generic for AES specifications. It consists of a number of different transformations applied consecutively over the data block bits, in a fixed number of iterations, called rounds. The number of rounds depends on the length of the key used for the encryption process.

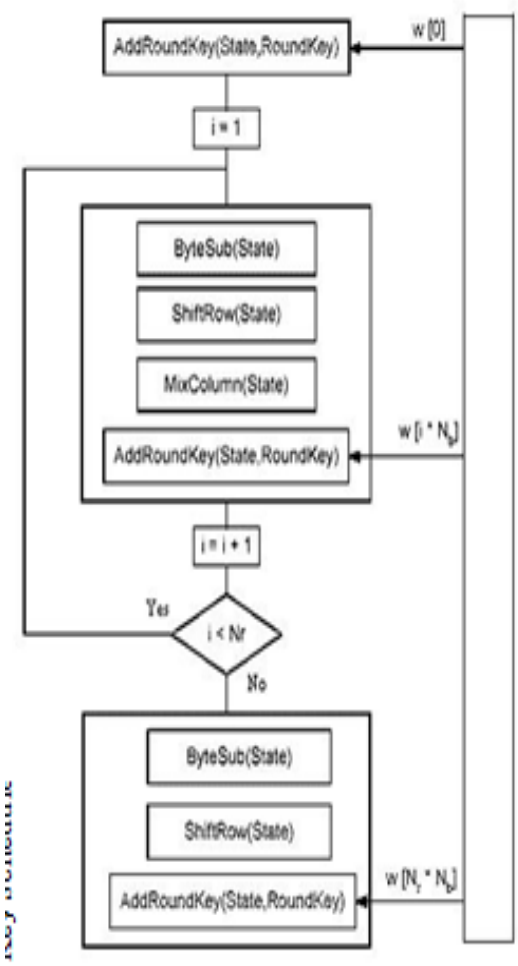

Figure 1. Encryption Process

3.1 Bytes Substitution Transformation

The bytes substitution transformation Bytesub (state) is a non-linear substitution of bytes that operates independently on each byte of the State using a substitution table(S-box) presented in figure7. This S-box which is invertible, is constructed by composing two transformations

4. DECRYPTION

The Decryption process of Advanced Encryption Standard algorithm is presented below, in figure 1. This process is direct inverse of the Encryption process (chapter2). All the transformations applied in Encryption process are inversely applied to this process. Hence the last round values of both the data and key are first round inputs for the Decryption process and follow0s in decreasing order.

1.1 Inverse Bytes Substitution Transformation

Inverse Byte Substitution Transformation InvSubBytes( ) is the inverse of the byte substitution transformation, in which the inverse S-Box (figure14) is applied to each byte of the State. This is obtained by applying the inverse of the affine transformation to the equation (16) followed by taking the multiplicative inverse in GF (2^8).

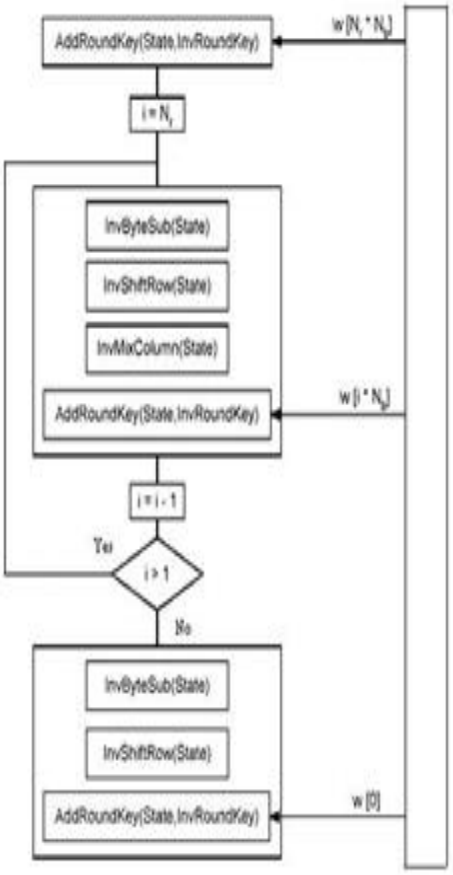

Figure 2. Decryption Process

5. CONCLUSION

Xilinx ISE tool has been used for the synthesis, place-and-route, and timing analysis. The pipelined implementation of the proposed design, we reach a clock cycle of 3.6182 ns (277.4 MHz of operative frequency). Once the function of individual modules is verified for correctness, these can be clubbed together. To support the above-mentioned approach, the crypto algorithm is split into two modules: coding and secret writing. The synthesis of the chip is performed within the XILINX tool targeting Xilinx Virtex 5 technology (XC5VLX30 target device) and therefore the

report is given in Table 1. The combination of Modelsim and Xilinx design flow has been used for the entire process. Individual register transfer logic (RTL) is obtained once synthesizing the VHDL style. The timing simulation is additionally performed to verify the functional correctness of the planning. However, the RTL diagram is not enclosed here for conciseness. The power analysis is performed using Xilinx's XPower analysis tool. The Virtex 5 Pro is a target device, as it is a full featured and flexible FPGA that contains two Power PC cores and plenty of logic cells and Devices,

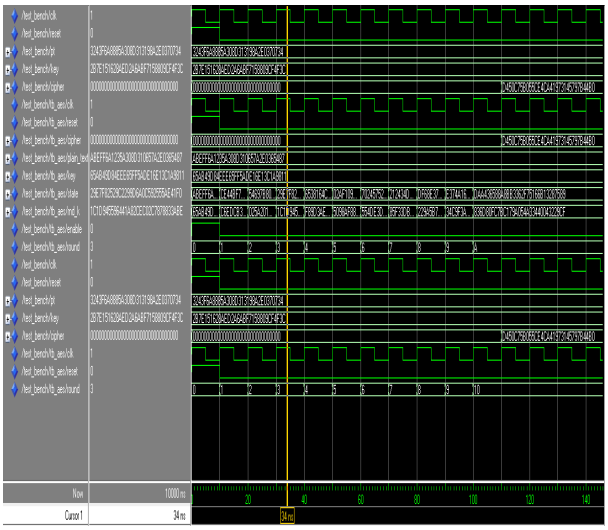

Figure 3. Simulation Result.

Device Utilization Summary			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Flip Flops	462	9,312	4%
Number of 4 input LUTs	3,510	9,312	37%
Number of occupied Slices	1,929	4,656	41%
Number of Slices containing only related logic	1,929	1,929	100%
Number of Slices containing unrelated logic	0	1,929	0%
Total Number of 4 input LUTs	3,745	9,312	40%
Number used as logic	3,510		
Number used as a route-thru	235		
Number of bonded IOBs	10	232	4%
Number of BUFGMUXs	1	24	4%
Average Fanout of Non-Clock Nets	5.46		

Figure 4. Device Utilization

I/O pin counts ranging from 208 to 1164 (Xilinx). It is set to run at 25 MHz during the simulations. Fig. 3 shows the simulation result forth encryption of a test vector. The design is synthesized in Xilinx Environment. The target device is xc5vlx30 in the family of Virtex5.Through the analysis of the schemes for throughput and power, it is evident that the proposed scheme outperforms the existing schemes. The standard national institute of standards and technology (NIST) and direct optimized routing(DOR) methodologies have been compared with the proposed technique. Table 2 compares the critical path, throughput, and power of the proposed technique with NIST and DOR techniques. The throughput of the DOR scheme is more comparing to the NIST scheme at the cost double number of required LUT slices for implementation. However, the proposed scheme provides the highest throughput of 277.4 Mbps with 31.8% reduction respectively in the LUT slices.

REFERENCES

[1] FIPS 197, "Advanced Encryption Standard *(AES)"*, November 26, 2001

[2] J. Daemen and V. Rijmen, "*AES Proposal:* Rijndael", AES Algorithm Submission, September 3, 1999

[3] ALTERA. Max+plus II VHDL. San Jose. Altera, 1996

[4] ALTERA "ACEX1K Embedded Programmable Logic Family Data Sheet", pdf files, (May 2003)

[5] ALTERA High-Speed RijndaelEncryption / Decryption Processors,

[6] Marcelo B. de Barcelos Design Case, "Optimized performance and area implementation of Advanced Encryption Standard in Altera

[7] "FPGA Simulations of Round 2 Advanced Encryption Standards"

[8] Tilborg, Henk C. A. van. "Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial", New York Kluwer Academic Publishers, 2002

[9] Peter J. Ashenden, "The Designer's Guide to VHDL", 2nd Edition, San Francisco, CA, Morgan Kaufmann, 2002