

**ABSTRACT**

The importance of cryptography applied to security in electronic data transactions has acquired an essential relevance during the last few years. In this work, an FPGA-based implementation of the Advanced Encryption Standard (AES) algorithm is proposed. The proposed design is developed on a soft-microcontroller (Microblaze) using hardware descriptive language (especially Verilog), Xilinx EDK environment. All the results are synthesized and simulated using Xilinx EDK, Xilinx ISE and ISim software respectively. An iterative looping methodology of block and key size of 128 bits is approached and also, S-box lookup table implementation is carried out which gives low latency, low complexity architecture and high throughput. The simulation results show the performance of the design.

**KEYWORDS:** AES, FPGA, encryption, decryption, block cipher, Microblaze, HDL

**INTRODUCTION**

In the current scenario, the encryption appears to be an inevitable part of any digital communication system to preserve both transmitted and received information. Encryption is the process by which the original information or text is converted into incomprehensible information commonly known as cipher text by applying a different type of computer algorithm. Among innumerable encryption algorithm, Advance Encryption Standard (AES) is mostly adopted by the U.S. Government Federal department for the safeguard of sensitive information. The specification of this AES is first published in 1997 by the National Institute of Standards and Technology (NIST) [1].

In general, the conventional encryption standards require a single independent key for both transmitting (encryption) and receiving (decryption) [2]. It is impossible to recover the original text from a cipher text without knowing the key. Hence, the security of encryption keys is very much essential. But the software implementation of the encryption key cannot be maintained all the time as the operating system itself prone to hacking. The other pitfalls of the software implementation include CPU design like instruction length, parallelism, mismatch in different operating system, etc. and also, sometime it cannot satisfy the speed required for a particular critical application. Hence, the above disadvantages lead to hardware implementation of the encryption algorithm which can provide more security, more speed and higher efficiency through parallelism. Fig.1 represents the general block diagram of an AES system.

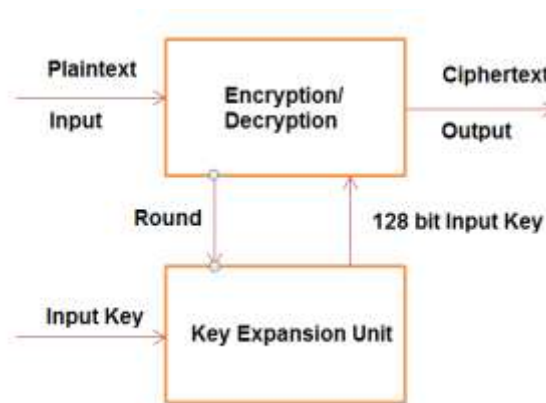


Fig. 1: Basic block diagram of AES

## RELATED WORK

In [3], a 32-bit datapath implementation in Spartan-3 is used in which low area, low power and low cost is achieved having throughput less than 1 Gbps. An optimized code for the Rijndael algorithm with 128-bit keys has been developed in [4] where the area and throughput are carefully trading off to make it suitable for wireless military communication and mobile telephony. In [5], Rijndael algorithm is implemented in a non-pipelined FPGA where all the key and data length combinations of the original Rijndael algorithm are supported and the maximum throughput of 1.19 Gb/s is achieved. The AES algorithm is programmed in VHDL and implemented on FPGA using an iterative design approach for the reduction of hardware consumption in [6]. Compact and Efficient Encryption/Decryption Module of the AES Rijndael is implemented on a single FPGA for Small Embedded Applications is described in [7] where a data stream of 208 Mbps is achieved and also it dealt with low area constraints. A new flexible AES architecture is explained that can perform both encryption and decryption with 128, 192, and 256 bit key options by a novel on-the-fly key generation module in [8] where the corresponding subkeys for encryption and decryption are generated concurrently and the architecture is simulated in Verilog HDL and implemented in FPGA and ASIC designs. In [9], the AES algorithm is investigated with regard to 256 bits message length and 192 bits key length and implemented in Spartan3 EDK pipelined architecture through the soft core processor Micro Blaze which is configured using System C coding. The design and implementation of a 128-bit Advanced Encryption Standard (AES) both symmetric encryption and decryption algorithm is explained by developing suitable hardware and software design on Xilinx Spartan-3E device in [10]. The system is further optimized in terms of execution speed and hardware utilization.

In this work, hardware implementation of the AES256 algorithm using the hardware description language (Verilog) on Microblaze (RISC Processor) based embedded system is proposed. The round keys generated which are consumed in different encryption iterations is the eccentric features of this design. In addition, the AES128 algorithm was modeled in "C" language. Finally, the performances of software and hardware implementations were compared.

## SOFT-CORE PROCESSOR FOR EMBEDDED SYSTEM DESIGN ON FPGA

There are a number of benefits to be gained from using soft processors on reconfigurable hardware (FPGA and Pro ASIC). For specific applications, the ability to update and up gradation embedded software in a device in the field has long been an advantage enjoyed by designers of embedded systems. With FPGAs, this has now become a reality for the hardware side of the design. For end-users, this translates as Field Upgradeable Hardware.

Microblaze, a soft microcontroller engine on Xilinx Environment for FPGA design, and it is a 32 bit RISC Machine for microcontroller with different Bus standard for intra system communication with flexible and programmable for general purpose & specify standard Implementation its development work. The MicroBlaze is a 32-bit Wishbone-compatible RISC processor, for use in FPGA designs targeting supported Xilinx Spartan or Virtex families of physical FPGA devices. MicroBlaze™ is the industry-leader in FPGA-based soft processors, with advanced architecture options like AXI or PLB interface, Memory Management Unit (MMU), instruction and data-side cache, configurable pipeline depth, Floating-Point unit (FPU), and much more. MicroBlaze is a 32-bit RISC Harvard architecture soft processor core that is included free with Vivado Design Edition, Vivado Webpack Edition and IDS Embedded Edition. Highly flexible architecture, plus a rich instruction set optimized for embedded applications, delivers the exact processing system you need at the lowest system cost possible.

MicroBlaze contains over 70 user-configurable options, enabling virtually any processor that is from a very small footprint, state machine or microcontroller to a high performance compute-intensive microprocessor-based system running Linux, operating at either 3-stage pipeline mode to optimize size, or 5-stage pipeline mode to optimize speed delivering faster DMIPs performance than any other FPGA-based soft-processing solution.

## DESIGN AND IMPLEMENTATION

The hardware and software requirements for work are Xilinx ML605 board, Xilinx SP605 board, or Xilinx Spartan®-3A Starter Kit, RS232 serial cable and serial communication utility (HyperTerminal), Xilinx Software Development Kit (SDK) 9.2, Xilinx Integrated Software Environment (ISE®) 9.2, Xilinx Embedded Development Kit (EDK) 9.2. The microcontroller first initially implemented for Spartan-3 architectures and can be modified to support other architectures. The entire embedded system is delivered as a netlist that can easily be instantiated into a Verilog or VHDL design, hence the need to create an EDK design [12].

Starting with ISE® Design Suite 9.2, MicroBlaze software development is fully supported by the standalone SDK, allowing C and C++ applications to be created and debugged without the need for EDK. The microcontroller comes pre-configured with two options: a UART option and a debug option. Once the code is debugged, the user can

switch netlists to reduce the size of the design. With a total of 3 files (2 for hardware implementation, 1 for software), a complete 32-bit MicroBlaze microcontroller can be added to any FPGA design.

The AES algorithm developed as an IP added to Microblaze based Embedded System environment system, which is built up in Xilinx EDK with PLB and MLB bus standard for internal communication, USART module is added to the external data communication with 9600 baud rate, BRAM and BRAM Controller is used for internal memory management in the process. The LEDs and Switch module are integrated for indicator and interrupt management of the process.

The BSB builder is used for the basic MicroBlaze environment for development, here the Spartan3E starter kit (Xilinx XC3S500E 320-pin FBGA package) board [11] is considered, and then an IP (AES) is added to the environment with consideration for internal and external communication. Fig. 2 shows the bus definition and width allocation. The AES process is developed in Verilog HDL, and then the address is generated and locked in later on stages as shown in fig. 3 and fig. 4. This integrated module is debugged in SDK environment, the debugging process is for a MicroBlaze based AES system which will communicate with USART module. The total module is simulated in Xilinx ISE environments using Isim Simulator and simulation result is shown in fig. 5.

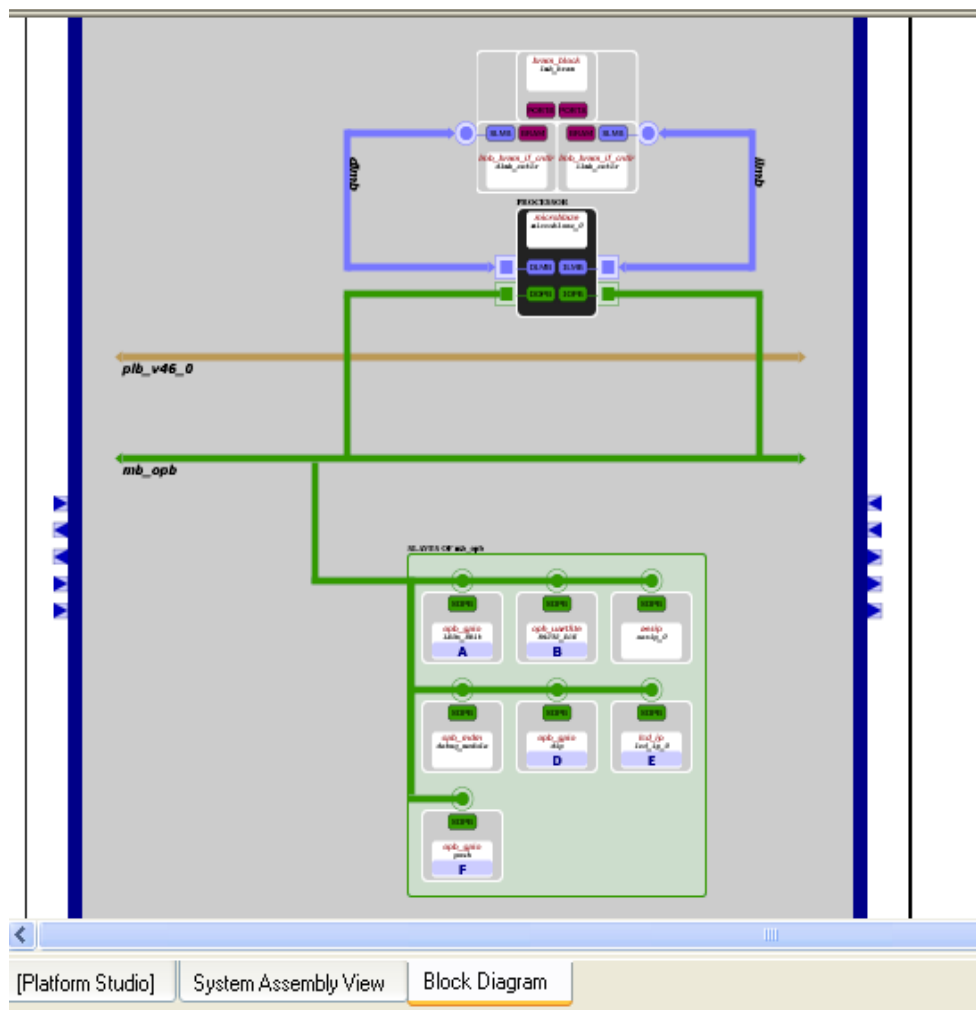


Fig. 2: Block Diagram of Microblaze with AES in Xilinx EDK

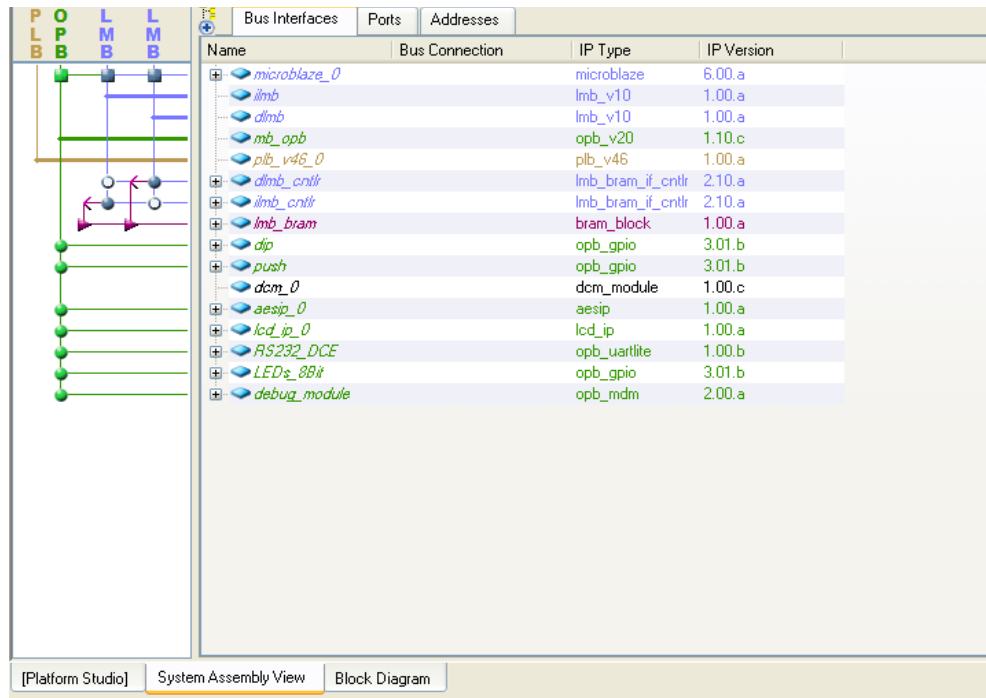


Fig. 3: Ports of Microblaze with AES in Xilinx EDK with respect to Spartan3E starter kit

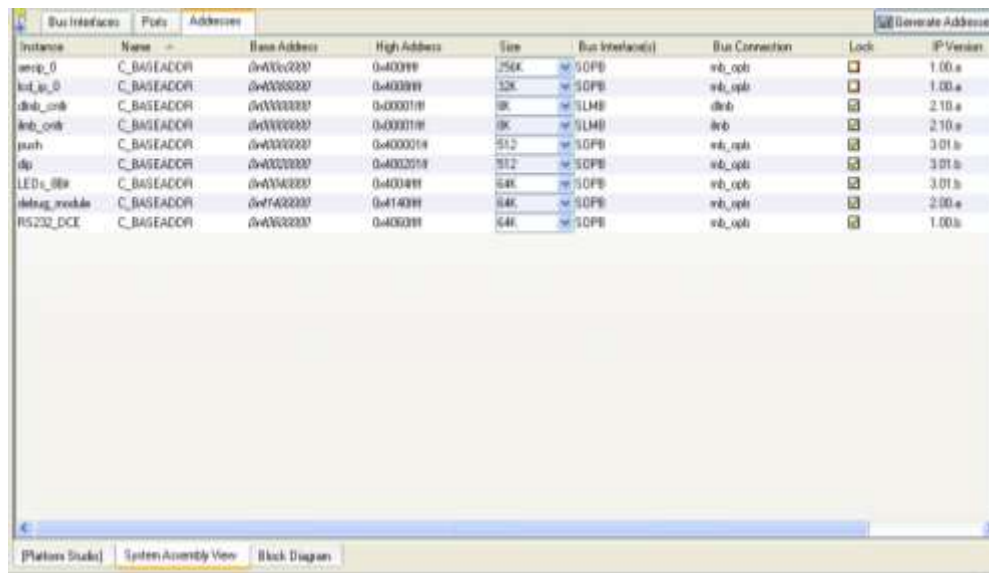


Fig. 4: Address of the port of Microblaze with AES in Xilinx EDK with respect to Spartan3E starter kit

Signal Name	Value
data_in[127:0]	>
key_in[127:0]	2b7e151628
iv_in[127:0]	0000000000
result[127:0]	d014f9a8c5f... d014f9a8c9ee2... 7649abac81... 5086cb9b50... d014f9a8c9ee25... 73bed6b8e3... 3ff1caa1681f...
golden[127:0]	0111001110
result_rd[127:0]	0101000010
iv_rd[127:0]	0000000000
key_rd[127:0]	1101000000
error_chk	0
i[31:0]	1111111111
error[31:0]	0000000000
AES_CR[3:0]	0000
AES_SR[3:0]	0001
AES_DIM[3:0]	0010

Fig. 5: Simulated Results in Xilinx ISE simulator



## CONCLUSION

In this paper the feasibility of creating a very compact, low-cost FPGA implementation of the AES is thoroughly examined. The proposed folded architecture achieves good performance and occupies less area than previously reported designs. This compact design was developed through examination of each of the components of the AES algorithm and matching them into the architecture of the FPGA. The designed core supports both encryption and decryption standards. By taking various inputs, its functionality has been verified using simulation, and is synthesized by using Xilinx 13.2. The design is targeted on FPGA (Spartan-3E).

## REFERENCES

- [1] Federal Information Processing Standards Publication 197, November 26, 2001, <https://www.google.co.in/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#>
- [2] H.S. Deshpande, K. J. Karande, A.O. Mulani, "Efficient Implementation of AES Algorithm on FPGA", Progress In Science in Engineering Research Journal, Vol.02, Issue January-February, pp.170-175, 2104
- [3] Chi-Wu Huang, Chi-Jeng Chang, Mao-Yuan Lin, Hung-Yun Tai, "Compact FPGA Implementation of 32-bits AES Algorithm Using Block RAM", IEEE, pp126, 2007
- [4] B.Jyrwa, R.Paily, "An Area-Throughput Efficient FPGA implementation of Block Cipher AES algorithm", IEEE, 2009
- [5] Refik Sever, A. NeslinI smailoglu, Yusuf C. Tekmen, Murat Askar, BurakOkcan, "A High speed fpga Implementation of the Rijndael Algorithm" Proceedings of the EUROMICRO Systems on Digital System Design, IEEE, pp.358-362, 2004
- [6] G. Rouvroy, Francois-Xavier Standaert, Jean-Jacques Quisquater and Jean-Didier Legat, "Compact and Efficient Encryption/Decryption Module for FPGA Implementation of the AES Rijndael VeryWell Suited for Small Embedded Applications", ITCC'04, IEEE, Vol.2, pp 583 – 587,2004
- [7] Atul M. Borkar, R. V. Kshirsagar, M. V. Vyawahare, "FPGA Implementation of AES Algorithm", IEEE, Vol-3, pp 401-405, 2011
- [8] H.Li, "Efficient and flexible architecture for AES", IEEE, Vol-153, Issue:6, pp 533 – 538, 2006
- [9] Santhosh Kumar. D, K.Navatha, Syed Mushtak Ahmed, "Implementation of AES Algorithm on Micro Blaze Processor in FPGA", IJARCC, Vol-2, Issue-10, 2013
- [10] M.Sambasiva Reddy, Y. Amar Babu, "Evaluation of Microblaze and Implementation of AES Algorithm using Spartan-3E", IJAREEIE, Vol-2, Issue 7, 2013
- [11] <http://www.xilinx.com/products/boards-and-kits/index.htm>
- [12] MicroBlaze Processor Reference Guide, Embedded Development Kit EDK 10.1i, UG081 (v9.0)

**AUTHOR BIBLIOGRAPHY**

	<p><b>Kaliprasanna Swain</b></p> <p>Working as Asst. Prof in the department of Electronics and Communication Engineering at G.I.T.A. Bhubaneswar, Odisha, India.</p>
	<p><b>Manoj Kumar Sahoo</b></p> <p>Working as Asst. Prof in the department of Electronics and Communication Engineering at G.I.T.A. Bhubaneswar, Odisha, India.</p>