Cryptographic Algorithms Implementation on RISC Processor

Y.Shekar, B.Vasunayak, J.Sunil Kumar, A.Sanyasi Rao, Fathima Shireen

Abstract—security is one of the most important features in data communication. Cryptographic algorithms are mainly used for this purpose to obtain confidentiality and integrity of data in communication. Implementing a cryptographic algorithm on a general purpose processor it results lower throughput and larger power consumption. In this work we propose processor architecture to perform the cryptographic algorithms and also it speed up the encryption and decryption process of data. This processor will perform the cryptographic operations as like general instructions in GPP. The data size of this processor is 32-bit. The architecture of the processor designed using Verilog HDL

Keywords: Cryptographic Algorithms, GPP, Verilog.

I. INTRODUCTION

There are two basic types of processors design philosophies: reduced instruction set computer (RISC) and complex instruction set computer (CISC). As the name suggests CISC systems use complex instructions. For example adding two integers is considered a simple instruction. But an instruction that copies an element from one array to another and automatically updates both array subscripts is considered a complex instruction. RISC systems use only simple instructions. RISC systems assume that the required operands are in the processors internal registers not in the main memory. A CISC design does not impose such restrictions. RISC designs use hardware to directly execute instructions.

Cryptography plays a significantly important role in the security of data transmission. On one hand with developing computing technology implementation of sophisticated cryptographic algorithms has become feasible. The cryptographic algorithms are classified into public key cryptography and private key cryptography. The private key cryptography which usually has a relatively compact architecture and smaller key size than public key cryptography is often used to encrypt/decrypt sensitive information or documents. Some well known examples of public key cryptographic algorithms are RSA (Rivest-Shamir-Adleman) and elliptic curve crypto systems and private key cryptographic algorithms are AES (Advance Encryption Standard), DES (Data Encryption Standard) and TEA (Tinny Encryption Algorithm). Implementation of these cryptographic algorithms on a general purpose processor is complex and also it has the drawback of lower throughput and higher power consumption.

Manuscript received November, 2013.

Y.Shekar, Department of E.C.E, Ganapathy Engineering College, Warangal, Andhra Pradesh, India

B.Vasunayak, Department of E.C.E, Ganapathy Engineering College, Warangal, Andhra Pradesh, India

J .Sunil Kumar, Department of E.C.E, Ganapathy Engineering College, Warangal, Andhra Pradesh, India

A.Sanyasi Rao, Department of E.C.E, BIES, Warangal, Andhra Pradesh, India

Fathima Shireen, Department of E.C.E, SREC, Warangal, Andhra Pradesh, India

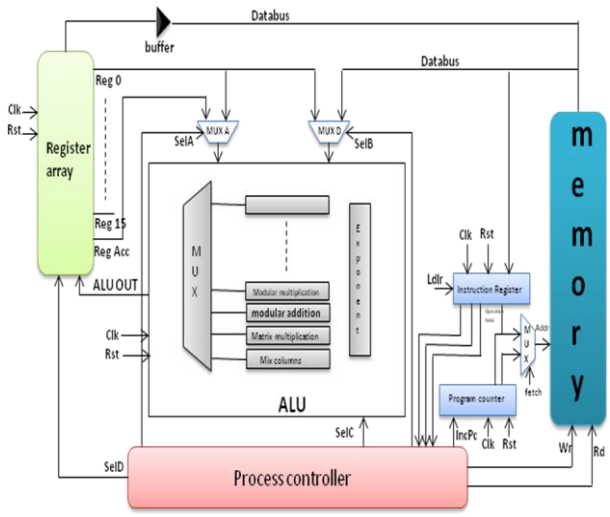
In the present work the design of an 32-bit data width RISC processor is presented based on cryptographic algorithms. It was designed with simplicity and efficiency in mind. It has a complete instruction set, Hayward architecture memory, general purpose registers and simple Arithmetical Logic Unit (ALU). Here the ALU design performs the cryptographic operations like operations in AES, Blowfish, IDEA algorithms. To design of RISC architecture we used Verilog HDL.

Present work is divided as follows: Section II presents the Processor architecture with cryptographic operations; section III presents the Cryptographic operations are presented; section IV is dedicated functional blocks and results discussions.

II. ARCHITECTURE OF PROCESSOR

The proposed processor has 32-bit data size, that its architecture has been designed in a way to be modular.

The ALU unit that uses a minimal instruction set, emphasizing the instructions used most often and optimizing them for the fastest possible execution. In this architecture the execution time of all instructions with the CPU clock cycle. The proposed architecture will perform both basic arithmetic and logical operations and cryptographic operations like Rotate word, Swapping, Fixed coefficient multiplication, matrix multiplication.



III. OPERATIONS OF CRYTOGRAPHIC

AES (Advance Encryption Standard) is a block cipher developed in effort to address threatened key size of Data Encryption Standard (DES). It allows the data length of 128 bits and different key lengths 128, 192, 256 bits. The main operations in AES are Shift Rows, Rotate Word, Matrix Multiplication, Mix column.

Blowfish is a symmetric block cipher that encrypts data in 8-byte blocks. The algorithm has two parts; key expansion and data encryption. Key expansion consists of generating

the initial contents of one array namely, eighteen 32-bit sub-keys and four arrays (S-Boxes), each of size 256 by 32 bits from a key of at most 448 bits. The main operations of this algorithm are addition modulo two (XoR) and addition modulo 2^32.

IDEA algorithm of the encryption process we provide the original (128 bits) cipher key to the mentioned unit. When the necessary the key generator unit produces different sub-keys by performing circular left shift operation by 25 bits on the current key and provides the sub-keys to other units. The unit named as multiplication modulo 216+1 is used to perform all the multiplication modulo 2^16+1 operation, when required the same unit is for bit wise Xor.

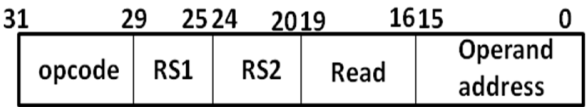
Instruction Set: for a complete design it was necessary to create a specific instruction set and its own instruction format. The instructions are classified in to Data manipulation and arithmetic logical operations.

The below table describes the complete instruction set. Each instruction having its own opcode.

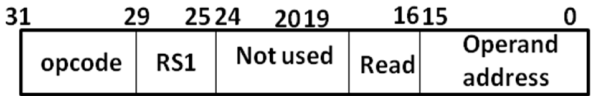
Syntax	Operation	Description
NoP	Nop	No operation
Ld Sr[A]	Sr= Memm[Address]	Move data from memory to register
Addition [A,B]	C=A xor B	GF(2m) addition
ModularMultiplication[A,B]	C=A+Bmod P	GF(2m) modular addition
Modular Multiplication[A,B]	C=A*Bmod P	GF(2m) modular multiplication
MatrixMultiplication [A,B]	Matrix multiplication	Polynomial matrix multiplication
Mix column[A,B]	C=Y*A mod X 4%1	Polynomial mix column transformation
Fixedmultiplier[A,B]	C=(03)*A	Reduction multiplication
AMXModulo [A]	C=A*(2A+1) mod P	Reduction modulo multiplication
Length rotation[A,B]	C=A<<B	Variable length rotation
Rotate word [A]	C=shiftrow(A)	Rotate word
LRShift[A,B]	C=A>>B,C=A<<B	Left, rotate shift operation

Table no.1

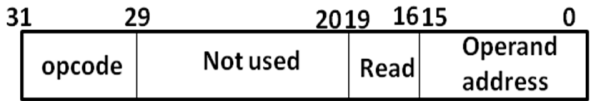
The logical operations like shift left, shift right and rotate word which requires only one source register shown in below type.



The operations like addition, modular functions require two source registers and to store result in destination result as shown in below type.



The load instructions and store instructions requires address from different data sources shown in below.



IV. RESULT DISCUSSION

Instruction Register: Instruction registers store the instruction which read from the memory and keep it as an output for the control circuit like operation code, source registers, operand address and operands these values set to general purpose registers.

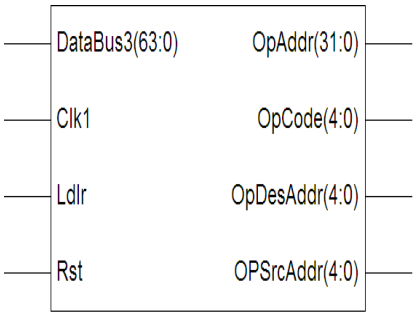


Figure no.2 Block diagram

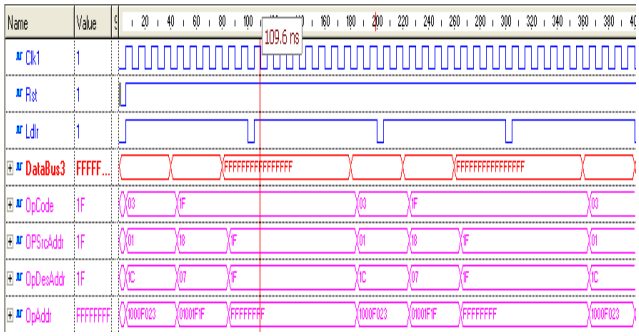


Figure no.3 simulation results

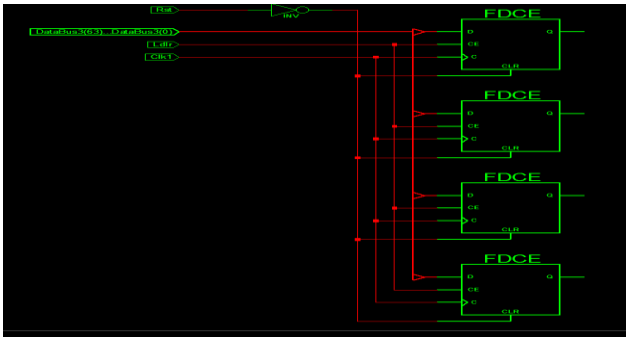


Figure no.4 Technology schematic

Logic Utilization	Usage	Availability
Slices	1	768
Flip Flops	47	1536
LUTs	1	1536
IOBs	93	124

Table no.2 implementation results

Arithmetic Logical Unit: The arithmetic logical unit has 16 operations each one of them was created and converted in to a symbol, and then a multiplexer was placed in order to obtain a 4-bit selector.

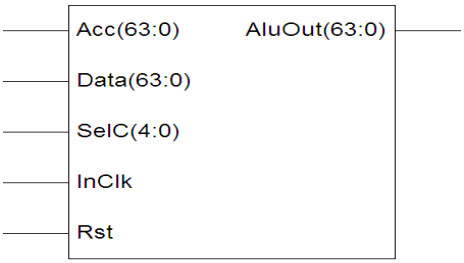


Figure no.6 block diagram

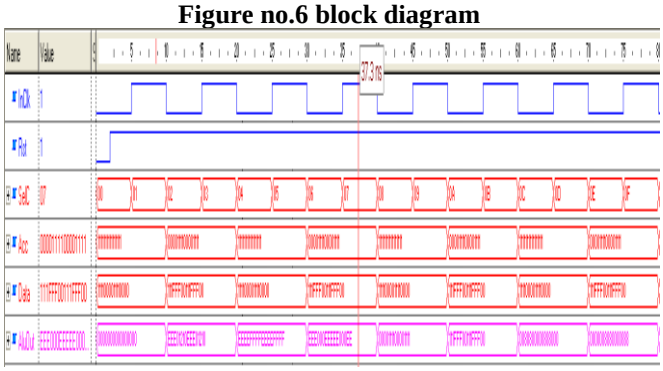


Figure no.7 simulation results

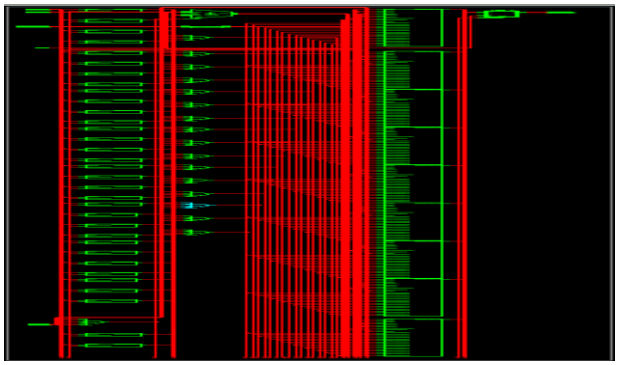


Figure no.8 Technology schematic

Logic Utilization	Usage	Availability
Slices	360	768
Flip Flops	64	1536
LUTs	652	1536
IOBs	199	124

Table no.3 implementation results

General Purpose Registers: General purpose registers store and save operands and results during program execution. ALU and memory must be able to write/read those registers so a set of sixteen 32-bit registers were used along with multiplexers and control circuit which are the operands to ALU which perform the operation.

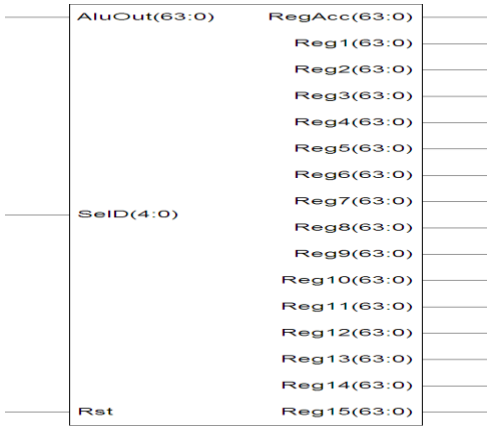


Figure no.10 block diagram

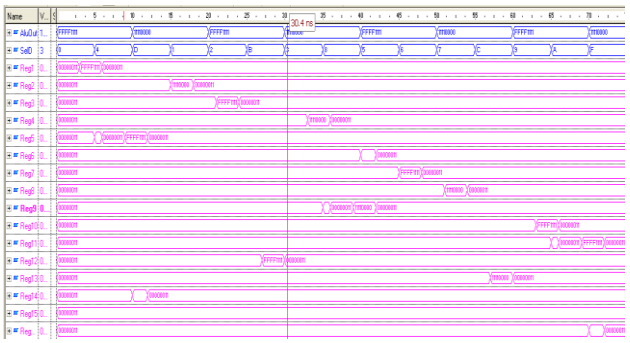


Figure no.11 simulation results

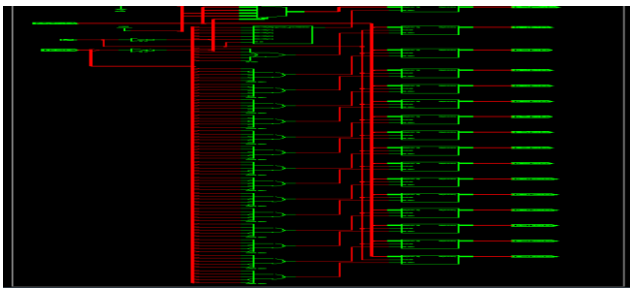


Figure no.12 Technology schematic

Logic Utilization	Usage	Availability
Slices	48	768
Flip Flops	87	1536
LUTs	1024	1536
IOBs	8	124

Table no.4 implementation results

Control Unit: The control unit is based on using FSM and we designed it in a way that allows each state to run at one clock cycle, the first state is the reset which is initializes the CPU internal registers and variables. The machine goes to the reset state by enabling the reset signal for certain number of clocks. Following the reset state would be the instruction fetching and decoding states which will enable the appropriate signals for reading instruction data from the memory and decoding the parts of the instruction. The decoding state will also select the next state depending on the instruction since every instruction has its own set of states, the control unit will jump to the correct state based on the instruction given.

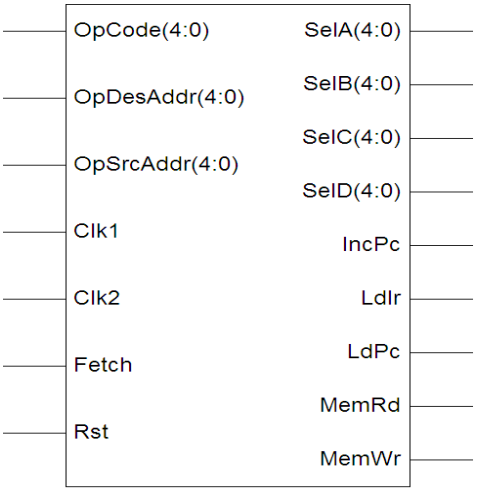


Figure no.13 block diagram

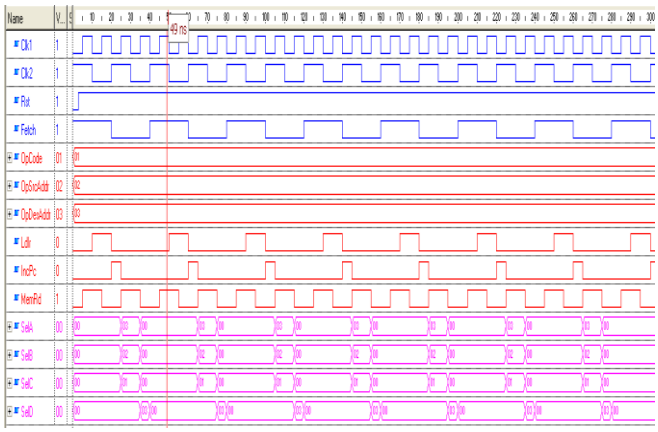


Figure no.14 simulation results

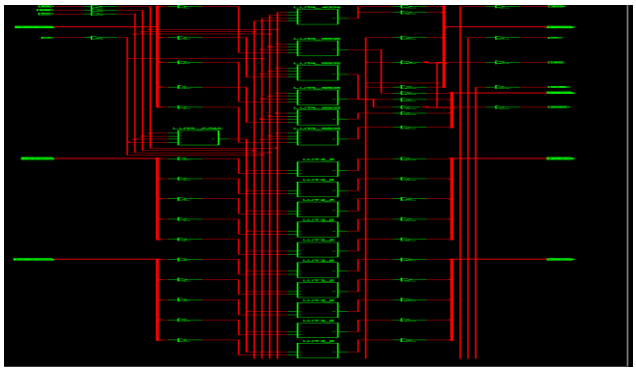


Figure no.15 Technology schematic

Logic Utilization	Usage	Availability
Slices	12	768
Flip Flops	44	1536
LUTs	20	1536
IOBs	44	124

Table no.5 implementation results

V.CONCLUSION

The 32-bit cryptographic processor performs mathematical computations used in symmetric key algorithms has been designed using Verilog HDL the simulations are performed using Active HDL and implementation performed using Xilinx tool.

REFERENCES

[1] Jun-hong chen "A High-Performance Unified Field Reconfigurable Cryptographic Processor". IEEE-2010

[2] Nima Karimpour Darav "CIARP: Crypto Instruction-aware RISC Processor.IEEE-2012"

[3] Antonio H. Zavala "RISC-Based Architecture for Computer Hardware Instruction" IEEE-2011

[4] "Data Encryption Standard" 1999 october 25.

[5] "Advance Encryption Standard" November 26 2001

[6] Imyong Lee, Dongwook Lee, Kiyoung choi, "ODALRISC: A Small, Low power and Configurable 32-bit RISC processor," International SOC design Conference 2008.

[7] Wayne Wolf, FPGA Based System Design, Prentice Hall, 2005.

[8] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES), (FIPPUB 197)", November 26, 2001, http://csrc.nist.gov/publications/.

[9] Atri. Rudra, Pradeep k. Dubey, Charanjit S.Jutla, Vijay Kumar, Josyula R.Rao, Pankaj Rahotgi, "Efficient Implementation of Rijndael Encryption with Composite Field Arithmetic," Proceedings of Cryptographic Hardware and Embedded Systems (CHES), Vol. 2162, pp.175-188, 2001.

[10] Rohit Sharma, Vivek Kumar Sehgal, Nitin Nitin1, Pranav Bhasker, Ishita Verma, "Design and Implementation of 64-Bit RISC Processor using Computer Modeling and Simulation," Proceedings of UKsim, Vol. 11, pp. 568 – 573, 2009.

[11] R. Uma, "Design and performance analysis of 8-bit RISC Processor using Xilinx tool," International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2, pp.53-58, March-April 2012, ISSN: 2248-9622.

[12] Jean-Luc Beuchat, "FPGA Implementations of the RC6 Block Cipher,'' Laboratoire de l'Informatique du arall´elisme, Ecole Normale Sup´erieure de Lyon,46, All´ee d'Italie, F–69364 Lyon Cedex 07.

[13] Arturo Diaz-Perez, Nazar A. Saqib, Francisco Rodriguez-Henriquez, ''Implementing Symmetric-Key Cryptosystems on Reconfigurable-Hardware,'' springer Nov 2006, ISBN : 0387338837.

[14] Imyong Lee, Dongwook Lee, Kiyoung choi, "ODALRISC: A Small, Low power and Configurable 32-bit RISC processor," International SOC design Conference 2008.

[15] R. Razdan and M.D. Smith, "A High-Performance Micro architecture with Hardware-Programmable Functional Units," Proceedings of. Micro-27, pp. 172-180, 1994.

[16] Vincent P. Heuring, and Harry F. Jordan, "Computer Systems Design and Architecture," Second Edition, 6th Dec, 2003, ISBN-10: 0130484407.

[17] Dave Van den Bout "The Practical XILINX Designer Lab Book," pp.30-31, ISBN 0-13- 095502-7.

[18] XILINX datasheet library, http:// www.xilinx.com/ partinfo/4000.pdf

[19] Jonas Thor, "Evaluation of a reconfigurable computing engine for digital communication Applications," pp.12-17, ISSN 1402-1617.

[20] Rasset T.L, Niederland R.A, Lane J.H, Geideman W.A "A 32-b RISC Implemented in Enhancement-Mode JFET Ga As," Vol.3, pp.60-70, 9 Oct 1986.

[21] Dolle.M, Jhand. S, Lehner.W, Muller.O, Schlett.M. "A 32-b RISC/DSP microprocessor with reduced complexity," Proceedings of journals and magazines, Vol. 32, Issue 7, pp 1056-1066, 06 August 2002.

[22] Buhler, M. Baitinger "VHDL-based development of a 32-bit pipelined RISC processor," U.G. Stuttgart University, Vol 1, pp. 138-142, 06 August 2002.

Yedunuri Shekar received the Bachelors Degree in Electronic & Communication Engineering from B I T S, Warangal (Andhra Pradesh, India) in 2010, Masters Degree in VLSI Design in 2013. I am currently working as Assistant Professor in Electronics & Communication Engineering Department, Balaji Institute of Engineering & Sciences, Warangal, India. His research interests include VlSI design, Signal processing, Embedded systems& Microprocessor

B.Vasu Nayak received the Bachelors Degree in Electronic Instrumentation & Engineering in 1999 from KITS, Masters Degree in Digital System and computer Electronics in 2011 from Vaagdevi Engineering College. He is currently an Assistant Professor with the Electronics & Communication Engineering Department, Ganapathy College of engineering, Warangal, India. His research interests include Microwave Engineering & Signal processing.

Jammala Sunil Kumar received the Bachelors Degree in Electronic Instrumentation & Control in 2004, Masters Degree in Digital Communication in 2007. He is currently an Assistant Professor in Electronics & Communication Engineering Department, Balaji Institute of Engineering & Sciences, Warangal, India. His research interests include Microwave Engineering & Signal processing.

Allanki Sanyasi Rao received his Bachelors Degree in Electronics & Communication Engineering in 1997, Masters Degree in Digital Systems & Computer Electronics in 2012. Totally he is having 15 years of teaching experience.
Currently he is Associate Professor and Head of the Dept. at Balaji Institute of Engineering& Sciences, Warangal, India. His research interests include Wireless communications, Signal processing and Network Security & Cryptography.

Fathima Shireen received the Bachelors Degree in Electronic & Communication Engineering from J I T S, Warangal (Andhra Pradesh, India) in 2009, Masters Degree in Embedded systems in 2013. I am currently working as Assistant Professor with the Electronics & Communication Engineering Department, Jaya Engineering College, Warangal, India. His research interests include VlSI design, Signal Processing, Embedded Systems & Microprocessor.