Volume 5, Issue 2, February 2015 **ISSN: 2277 128X**

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementation of Secured MIPS Pipeline Processor using RC6 Algorithm with Vhdl

Vishaka Ambardar*
Student Vlsi design, GNDEC
Ludhiana, India

Dr. Munish Rattan
ECE Department, GNDEC
Ludhiana, India

Abstract— This paper presents the design and implementation of a RC6 algorithms based Crypto Processor containing both encryption and decryption processes in the same design. The Crypto Processor architecture is divided into different modules and every module is implemented individually. The hardware design is implemented using Xilinx devices. The main parts of ALU module and Permutation Module in HDL descriptions are related with the transformations of Rivest Cipher-6 crypto algorithm, are compiled into hardware using the Xilinx and HDL EASE tool. Testing results shows that the MIPS crypto processor operates successfully.

Keywords— MIPS Processor, Reduced Instruction Set Computer (RISC), VHDL, Pipeline, Xilinx 12.3, FPGA

I. INTRODUCTION

Cryptography is an art of protecting information by changing it into an unreadable format. Encryption is emerging as a vital part in the transmission of data. Encryption is the process of converting plain data (known as plaintext) into intangible data (known as cipher text) through an algorithm referred to as cipher. This achieves various goals of security like Authentication, Confidentiality Integrity and Non-repudiation. Under this process it is essential to prove one's identity and then ensures that the message can only be read by the intended receiver.

A standard feature of Pipelining is an implementation technique used to improve both CPI (Cycle Per Instruction) and overall system performance [1]. Pipelining allows a processor to work on different steps of the instruction at the same time, thus more instruction can be executed in a shorter period of time. Thus in pipelining each module of MIPS processor does not wait for the previous instruction to finish before it can execute. Pipelining the MIPS processor introduces events called hazards [1], which prevents the next instruction in the instruction stream from being executing during its designated clock cycle and reduce the speed of the processor.

The MIPS instruction set is straightforward like any other RISC designs. MIPS are a load/store architecture, which means that only load and store instructions access memory. Other instructions can only operate on values in the registers [2]. Generally, the MIPS instructions can be broken into three classes: the memory-reference instructions, the arithmetic-logical instructions, and the branch instructions.

The MIPS is simply known as Millions of instructions per second and is one of the best RISC (Reduced Instruction Set Computer) processor ever designed. MIPS architecture is employed in a wide range of applications. The architecture remains the same for all MIPS based processors while the implementations may differ [3].

These five pipeline stages processor generate 5 clock cycles processing delay and several Hazards during the operation [2]. These pipelining Hazard are eliminates by inserting NOP (No Operation Performed) instruction which generate some delays for the proper execution of instruction [1].

The types of hazards include structural, data and control hazards.

1) *Structural hazards* arise when the flow of instructions requires more hardware resources than those available on the platform [4].

2) Data hazards arise when there is a data dependency between the current instruction and the previous instruction in the pipeline.

3) Control hazards arise when there is a change in the flow of the program (branch instruction that changes the PC).

II. ALGORITHM USED

A. RC6 Algorithm

Many modern processors have constant-time rotation and multiplication instructions. Other processors may have a rotation or shift time that depends linearly with the amount of rotation, but in this case it is usually easy to arrange the work so that the total compute time is data-independent (for example, by computing a rotate of t bits using a left-shift of t bits and a right-shift of w-t bits). RC6 can easily be implemented in such a way as to be invulnerable to “timing attacks". In either case, the RC6 encrypt/decrypt time is data-independent, causing any potential timing attacks to fail.

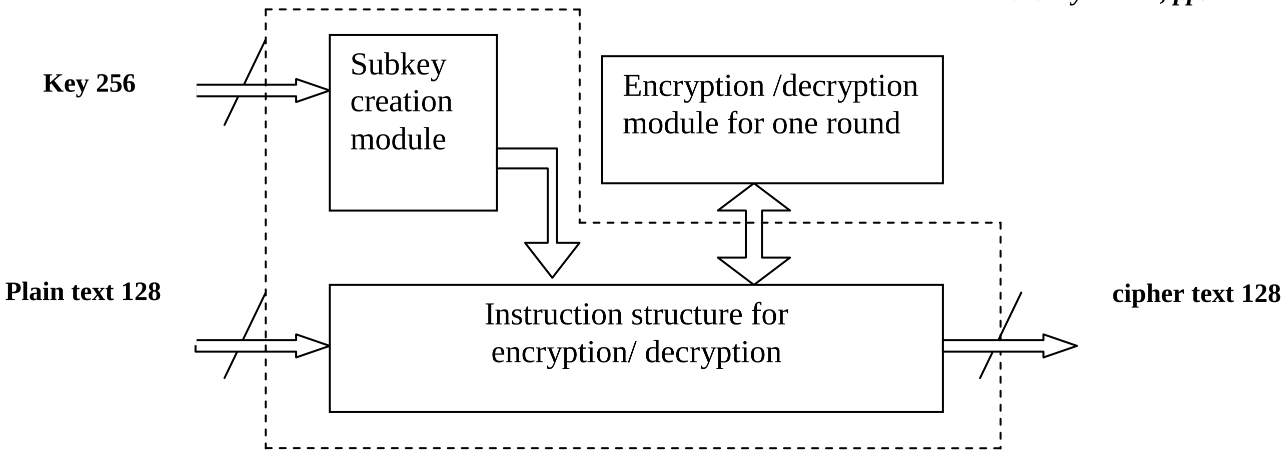
Key 256
Subkey creation module
Encryption /decryption module for one round
Plain text 128
Instruction structure for encryption/ decryption
cipher text 128

Fig. 1 The Encryption/Decryption Circuit

RC6 works with four w-bit registers A, B, C, D which contain the input plaintext as well as the output cipher text at the end of encryption. The first byte of plaintext is placed in the LSB of A, the last byte of plaintext is placed into the MSB of D. We use (A, B, C, D) = (B, C, D, A) to mean the parallel assignment of values on the right to registers on the left. Fig 2 show the RC6 algorithm

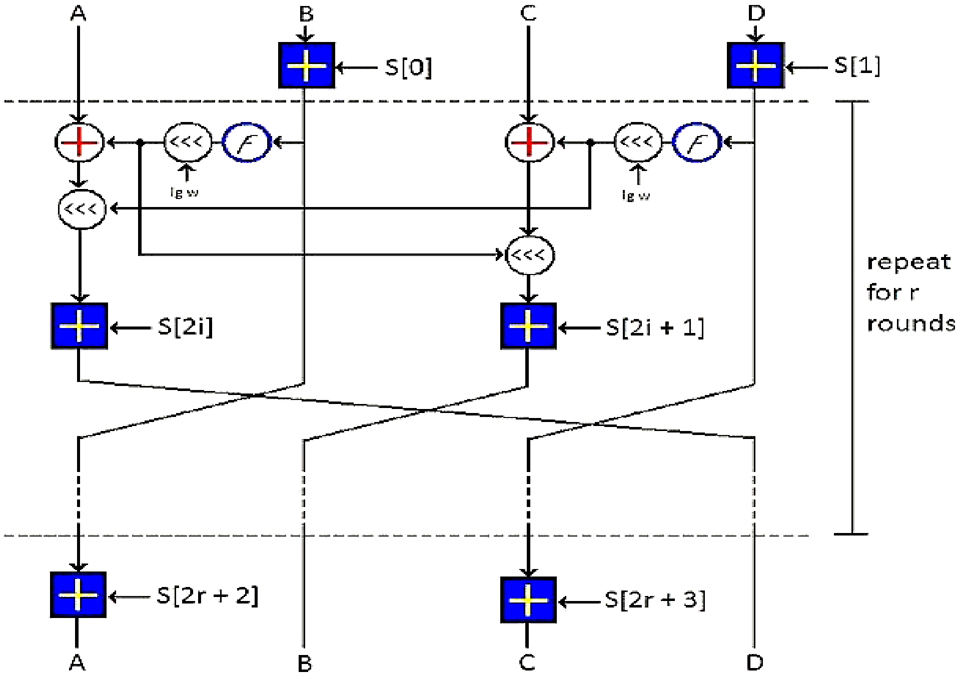

Fig :2 RC6 Algorithm

III. METHODOLOGY

A. MIPS crypto processor architecture

The main operation in RC6, DES and TDES is bit permutation and substitution in one round which is performed by the permutation unit. Data path processing unit performs the 5 stages pipelining process inside the processor.MIPS crypto processor (shown in Fig. 3) consists of various components like Datapath, Data I/O unit, Control Unit, Memory unit, Crypto Specific Unit, Dependency Resolver and Arithmetic Logic Unit. The dedicated data processing block consist of Datapath and Crypto IP core (coprocessor). At every positive edge clock cycle the program counter unit updates the values available at its input bus and also fetches the next instruction from the instruction ROM memory. Opcode is passed to the control unit which asserts the required control signals. Sign extension is used for calculating the effective address. The MIPS controller is the main core of the architecture which consists of control unit and ALU control signal unit. The controller controls the crypto block and performs the interface and dedicated operation with the external devices such as Memory, I/O bus interface controller. The Load and Store instructions write to and read from the RAM memory in the memory unit while the ALU results and the data read from RAM are written in to the register file by the register type and Load instruction respectively. The dependency resolver block has a function to avoid stall by rearranging the instruction sequence and checking the successive instruction for their stall possibility by comparing their operands[6]. This module handles both stalling as well as data forwarding of previous stage. In case of data dependency between two consecutive instructions the receiving instruction waits for one clock cycle.

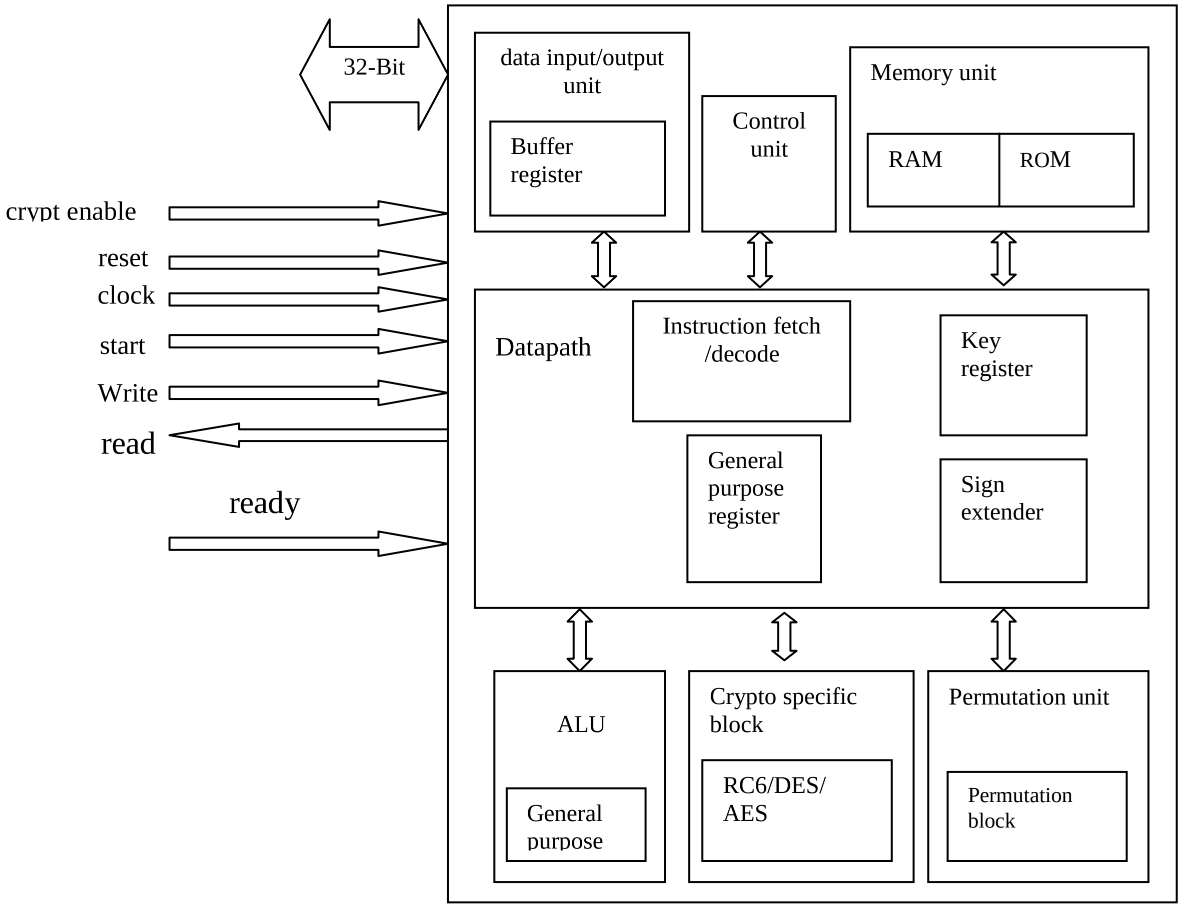

Fig 3: MIPS Crypto Processor Architecture

B. Pipelined MIPS CPU

The pipeline structure of the processor is a modified version of a popular load/store RISC [4]. The basic pipeline for a MIPS integer unit contains 5 stages:

1) Instruction fetch (IF) It fetches the next instruction. First, it sends the contents of the PC register, to the instruction memory. The instruction memory will then respond by sending the correct instruction. This instruction is sent on to the instruction decode. The instruction decode phase will calculate the next PC and will send it back to the IF Instruction.

2) Decode (ID) The main function of the instruction decode unit is to use the 32-bit instruction provided from the previous instruction fetch unit to index the register file and obtain the register data values. We must simply calculate PC+4 to get the address of the next instruction.

3) Execution (EX) The execution unit of the MIPS processor contains the arithmetic logic unit (ALU) which performs the operation determined by the ALU op signal. The Execution phase "executes" the instruction. Any calculations necessary are done in this phase.

4) Memory access (MA) The purpose of the Memory access phase is to store operands into memory or load operands from memory. So, for all instructions except loads and stores, the MA simply passes on the value from the ALU on to the WB stage (12, 16). For loads and stores, the MA needs to send the effective address calculated by the ALU to memory.

5) Write back (WB) The Write Back phase, finally, is a very simple one. It simply takes the output of the MA phase and sends it back to the write back phase to store the result into the destination register.

IV. RESULTS

The complete pipeline processor stages are modeled in VHDL. The syntax of the RTL design is checked using Xilinx tool. For functional verification of the design the MIPS processor is modeled in Hardware Descriptive Language. The design is verified both at the block level and top level.

Table 1 Result summary for Crypto Processor

Features	**Processor**
Target Device	Virtex-6 (XC6vlx240t-3ff1156)
Technology	40nm
Crypto processor	RC6
Data length	128-bits

Speed	218MHz (clock rate)
Throughput	664 Mbits/s (Data Bandwidth)
Key Setup	188 clock cycles in 4305ns
Reading Input	1clock cycle in 22.87ns
Area	66072 Slice LUT's(look up tables)
Latency	21 clock cycles(both for encryption and decryption)
Power consumption	1.746W(quiescent-1.303 and dynamic-0.444)

Table-2 Comparison betweenRC6,AES and TDES Crypto Processor

PARAMETERS	RC6	AES	TDES
Speed	218MHz (clock rate)	210MHz (clock rate)	209MHz(clock rate)
Area	66072 slice LUT's	109738 slice LUT's(look up tables)	64673 slice LUT's(look up tables)
Throughput	664 Mbits/s (data bandwidth)	560Mbits/s (data bandwidth)	636 Mbits/s (data bandwidth)
Latency	21 clock cycles	48 clock cycles	21 clock cycles
Power consumption	1.746w	1.313w	1.981w

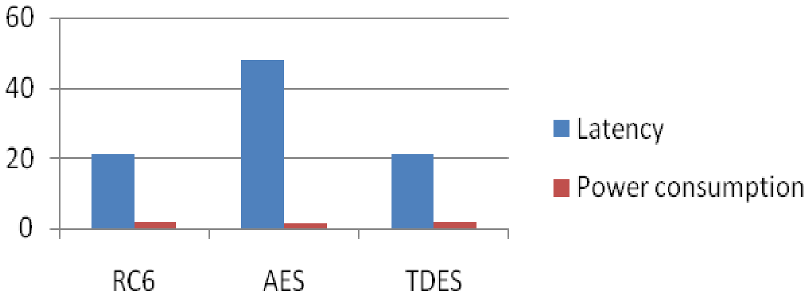

Fig 4: Comparison of three algorithms on basis of Latency & Power consumption

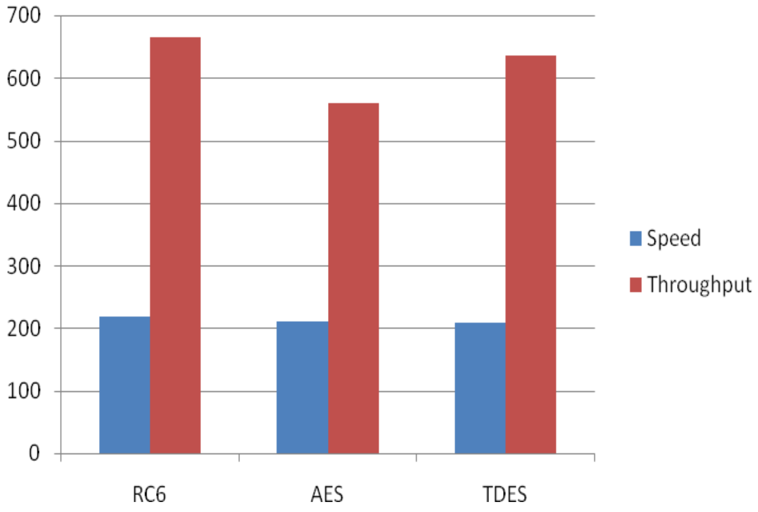

Fig 5: Comparison of three algorithms on basis of Speed & Throughput

V. CONCLUSION

RC6 algorithm method is proposed for the MIPS Architecture Cryptography. Initially the basic MIPS architecture is taken and crypto cores are implemented on basis of RC6 algorithm.

By this the data inside the processor became more secure and threat proof .The system became more robust as the data transaction has become more reliable. So whenever the data is required in crypt form, this algorithm is best suitable.

The design has been modeled in VHDL and functional verification policies are adopted for it. Optimization and synthesis of design is carried out at latest and fastest FPGA Viretx-6 device that improves performance. Every instruction is tested with some of vectors provided by MIPS. We conclude that the performance on bases of speed and throughput of MIPS crypto processor using RC6 is high and reliable.

REFERENCES

[1] David A. Patterson, John L. Hennessy, “Computer Organization and Design - The Hardware/Software Interface” Second Edition (1998) Morgan Kaufmann Publisher, Inc.

[2] Rupali S. Balpande, Rashmi S. Keote.2011, “Design of FPGA based Instruction fetch & decode Module of 32-bit RISC (MIPS) processor”, International Conference on communication Systems and Network Technologies, IEEE, ISBN: 978-0-7695-4437-3, pp.409-413, 2011.

[3] Kirat Pal Singh, Shivani Parmar,“Low Power Encrypted Mips Processor Based On Aes Algorithm”,Vlsi Design Department Academic & Consultancy Services Division Centre for Development of Advanced Computing (C-DAC) , Mohali-160071, Journal of Global Research in Computer Science Volume 3, No. 4, 2012

[4] Galani Tina, R.D.Daruwala,“Performance Improvement of MIPS Architecture by Adding New Features,” Department of Electrical VJTI College of Engg, Mumbai India ,International Journal of Advanced Research in Computer Science and Software Engineering Research Paper, ISSN: 2277 128X Volume 3, Issue 2, ,2013

[5] Kirat Pal Singh, Dilip Kumar,” Performance Evaluation of Low Power MIPS Crypto Processor based on Cryptography Algorithms” Vlsi Design Department Academic & Consultancy Services Division Centre for Development of Advanced Computing (C-DAC) , Mohali-160071, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, , pp.1625-1634 1625,2012

[6] Verma H.K.,R.K. Singh, “Enhancement of RC6 block cipher algorithm and comparison with RC5 & RC6” Advance Computing Conference (IACC), 2013 IEEE 3rd International DOI: 10.1109/IAdCC.2013.6514287, pp 556 - 561 , 2013

[7] Mohamed A.B., Zaibi, G., Kachouri, A,”Implementation of RC5 and RC6 block ciphers on digital images”, 8th International Multi-Conference on Systems, Signals and Devices (SSD),DOI: 10.1109/SSD.2011.5767447 , pp 1 – 6, 2011

[8] Megalingam, Rajesh Kannan ; Joseph, I.P. ; Gautham, P. ; Parthasarathy, R. ; Deepu, K.B. ; Nair, “Reconfigurable Cryptographic Processor for multiple crypto-algorithms ,” M.M. Students' Technology Symposium (TechSym), 2011 IEEE DOI: .1109/TECHSYM.2011.5783846 , pp 204 – 210, 2011

[9] Gautham P, Parthasarathy R, Karthi Balasubramanian., “Low-power pipelined MIPS processor design”, International symposium on integrated circuit (ISIC’09), pp. 462-465,2009.

[10] Zulkifli, Yudhanto, Soetharyo and adinono., “Reduced Stall MIPS architecture using Pre-fetching accelerator”, International conference on electrical engineering and informatics, IEEE, ISBN: 978-1-4244-4913-2, pp. 611-616, Aug. 2009.

[11] Pravin B. ghewari, Mrs. Jaymala K. patil, Amit B. Chougule., “Efficient hardware design and implementation of AES cryptosystem”, International journal of engineering science and technology, ISSN: 0975-5462, Vol. 2(3), pp. 213-219, 2010.