International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 4, No. 3, November 2015, pp. 185~191
ISSN: 2089-4864

NIOS II Based Secure Test Wrapper Design for Testing Cryptographic Algorithms

Chakrapani Kannan
Shanmugha Arts, Science, Technology & Research Academy (SASTRA University)
Thanjavur, Tamil Nadu 613401, India

Article Info

Article history:

Received May 6, 2015
Revised Jul 19, 2015
Accepted Aug 7, 2015

Keyword:

Cryptographic algorithms
NIOS II
Soft-core processors

ABSTRACT

Cryptographic algorithms need infrastructure for testing them against security attacks. Normally many methods are proposed for testing these cryptographic primitives. Normal designs cannot be applied to all types of cryptographic chips. Usually build in self test is applied for the intellectual property chips for testing them. But it suffers from many problems such as side channel attack, backholes, high area overhead, etc.., to overcome all these drawbacks test wrapper is designed and tested using NIOS II economy soft core processor. NIOS II is utilized as the soft core processor and cryptographic algorithms are executed. RTL view of these cryptographic circuits is described. Synthesis result shows the chip planner view of the circuits and the area required for the logic elements. NIOS II soft-core processors perform well for testing the cryptographic algorithms. Results with respects to area optimization, memory and speed are discussed. The logic components required for design using NIOS II is optimized. Memory required is also less compare to other processors. Area required is optimized using NIOS II processor and it is flexible for design of complex circuits.

Corresponding Author:

Chakrapani Kannan
Shanmugha Arts, Science, Technology & Research Academy (SASTRA University)
Thirumalaisamudram, Thanjavur, Tamil Nadu 613401, India
Email: kcp@core.sastra.edu

1. INTRODUCTION

Advancement in internet technologies has increased the need for protection of data and information now a day. Cryptographic algorithms plays important role in protecting these data among the increasing attacks. Evaluation of Cryptographic algorithm in any chip is very important to ensure the security for which application they are intended to perform. These cryptographic algorithms are already proven with their mathematical model. Though they are secure enough in the computational techniques it is important to prove them as secure for implementing with an intellectual property (IP) core or a chip. High speed testing is required to achieve highest testability regarding the faults in chips which are unattended. Security is an important factor when designing any IP core. In the present world due to many advancement and inventions in the IP cores it is very difficult to find the appropriate IP core for any application and testing them is also become a crucial factor. Wrappers are used for testing this IP cores in terms of their feasibility, faults, performance evaluation, etc. Wrappers are piece of software coding which is required for testing IP cores. These wrappers will work as a test pattern or test sequence for testing the IP cores or any chip. Here in this work NIOS II soft-core processor is used for testing the IP cores. NIOS II works like a wrapper for testing the cryptographic algorithms against all kind of attacks. NIOS II economy processor is used which uses only fewer logic and cheaper in cost among other processors. As it has fewer logics execution time is reduced and high performance is achieved using these processors.

In this paper various cryptographic algorithms are tested among the NIOS based soft-core processors. These performances are discussed and the effective result analysis is made among the algorithms. The work flows as section II describes the previous work done on the wrapper design , section III presents the various cryptographic algorithms and there primitives. In section IV synthesis results are discussed and finally the conclusion is drawn in section V as the paper flows.

2. PRIOR WORK

System on chip (SOC) is nothing but the chip which integrates the processors, memories and interfaces devices in the form of core IC. Testing this SOC are major constrain in the 1999 and then later technologies are invented for testing IP cores. Test access machine (TAM) and test wrappers are invented for testing the core processors. Test wrappers are very important as they minimize the idle time taken for testing the cores with vectors. This in turns also reduce the memory requirement for vector in the chip. Wrappers have many operation modes such as normal, core, interconnect and bypass test.

A wrapper named Test collar [4] was invented which is used for testing core in the past. But the interconnect test is not performed using this wrapper. Balanced wrapper chain is used which consist of cores in chain and has internal scan which reduces the time taken for scanning [5]. There are many types of wrappers are been designed in the literature such as core transparency [6], multiplexed access [7]. All these wrappers designs address some problem but still have some constrains along with the modifications.

In this paper we have tested the wrapper using NIOS II economy soft core processor for various cryptographic algorithms. The time taken for these algorithm to execute are also been discussed. Wrapper performance is analyzed in this work.

3. FUNCTIONAL DESCRIPTION

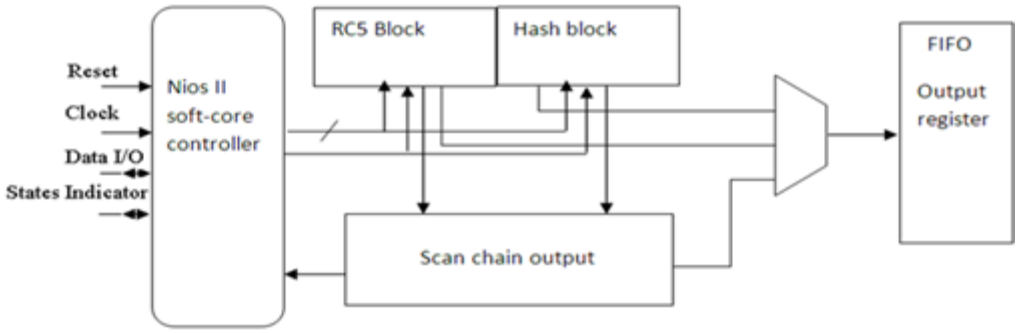

Figure 5.1. Functional block diagram of NIOS II processor

The figure 5.1 gives the functional block diagram of NIOS II soft core processor based wrapper design. NIOS II processor is given with control and data inputs. The RC5 block and Hash block will generate certain test output for the given input data set. The outputs from these blocks are given to these scan chain output where it compares and gives back the output to the processor for comparing with the input. Simultaneously output for the given input sequence is given to the output register for verification. If the input generates the expected output then the hardware performance is appropriate. NIOS II based soft core processor performs well for this type of wrapper based testing of test sequences. In this work cryptographic algorithms are tested on NIOS II processor.

NIOS II based soft-core processors are very flexible and suitable for testing circuits with different test sequence simultaneously. If any change in the hardware model of the proposed system can be easily modifies by changing few commands. Modification of the hardware can be easily reflected with NIOS II based soft-core processor. These processors utilize very less logic components when compared to other processors. Hence speed increases with less area utilization in NIOS II soft-core processors. This decreases the complexity in computation of any circuits including complex cryptographic designs.

4. CRYPTOGRAPHIC ALGORITHMS

In the present and literature many cryptographic algorithms are invented for secret data communication in case of any critical applications. Cryptographic algorithms used to authenticate the information and to keep information as private. Algorithms are used for transformation of original information into some other form for transmission and again retrieving the original host message at the receiver side. It is impossible for everyone to create their own cryptographic algorithms for their applications. There are many algorithms already existing patented and used for a long time. Any cryptographic algorithm which is secure for a long time in the public scrutiny can be used for secure data communication. Most of the cryptographic algorithms consist of many rounds of encryption function to increase the efficiency and security of the algorithm. When these algorithms are integrated for intended applications along with the data increases the computational complexity.

In this work algorithm which are proven to be secure in the public scrutiny for a long time has been taken. These algorithms are tested in the wrappers based on NIOS II processor. The performance, time taken for execution, efficiency is to calculated using test wrappers. Performance analysis based on the test wrappers are evaluated for AES encryption, RC5, SHA 5 and ALU is implemented for its performance analysis.

5. AES ENCRYPTION

Advanced Key Encryption (AES) is a private key encryption technique used from a long time. This algorithm uses different key with different block size. Each block in this technique has a block length of 128 bit with different key length. It is a symmetric key algorithm which uses same key for encryption and decryption. Four stages of block cipher are used for deriving key in this encryption algorithm. Adding round key at the first stage then three consecutive rounds are subbytes, shiftrow, mixcolumns will take place. This round key process is repeated for many iterations and reverse of same will be the decrypting process. Figure 1 shows the schematic for AES encryption.

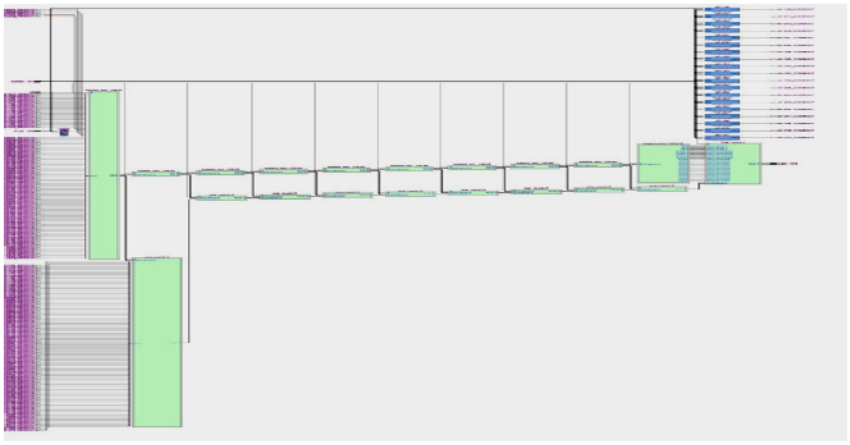

Figure 1. Schematic for design of AES algorithm

6. RC5 ALGORITHM

RC5 is a block cipher symmetric key encryption which is very simple than other cryptographic algorithms. This algorithm has variable size of blocks according to the application. Number of rounds for encryption also varies from 0 to 255 accordingly. Feistel like structure with number of exclusive OR and modular additions are used in the RC5 encryption technique. In RC5 key is very important, encryption and decryption are few commands. Algorithm is data dependent rotations in its encryption and decryption process. 64 bit key is used for encryption in RC5 algorithm. The figure 2 shows the schematic of RC5 algorithm.

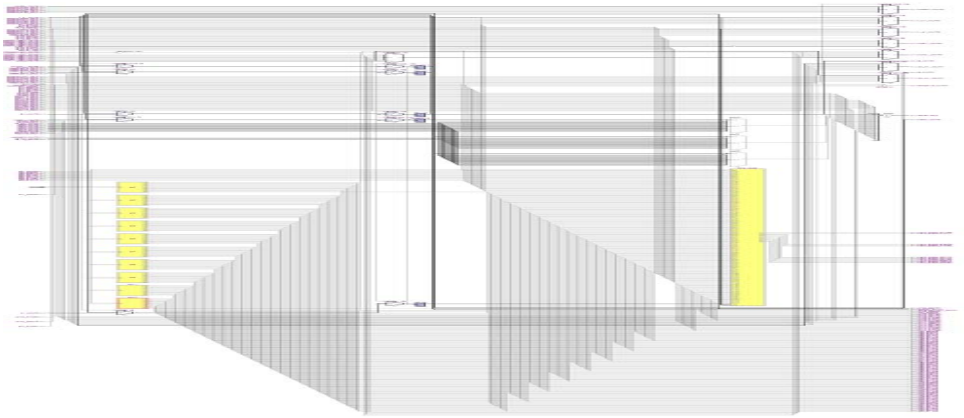

Figure 2. schematic view of RC5 algorithm

7. HASH ALGORITHM

Secure hash algorithm (SHA) is a cryptographic hash function which is mostly used in case of the integrity check. These cryptographic hash functions are difficult to rebuild or construct again in reverse engineering process thus provide high security for the data. These hash functions have their applications in information security, digital signatures, message authentication codes and other forms of authentications. Important quality of hash functions are the pre and second image resistance. Resistance against the collision is another important factor. Figure 3 shows the RTL view of SHA algorithm.

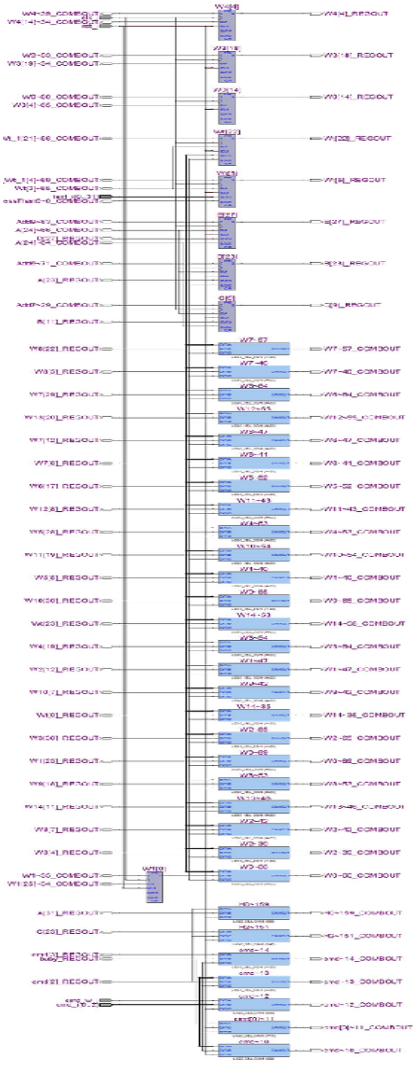

Figure 3. RTL view of HASH Algorithm

8. ALU

Arithmetic logic unit is a digital circuit which will perform the arithmetic and logical operations. It is the basic block for functioning of central processing unit. The performance of ALU will determine the speed of the processor or the digital design. The ALU will perform all the logical operations and depending on the ALU performance cryptographic algorithms will be executed as they depend on ALU for numerous logic OR and EXOR operations. Figure 4 dhows the RTL view of ALU.

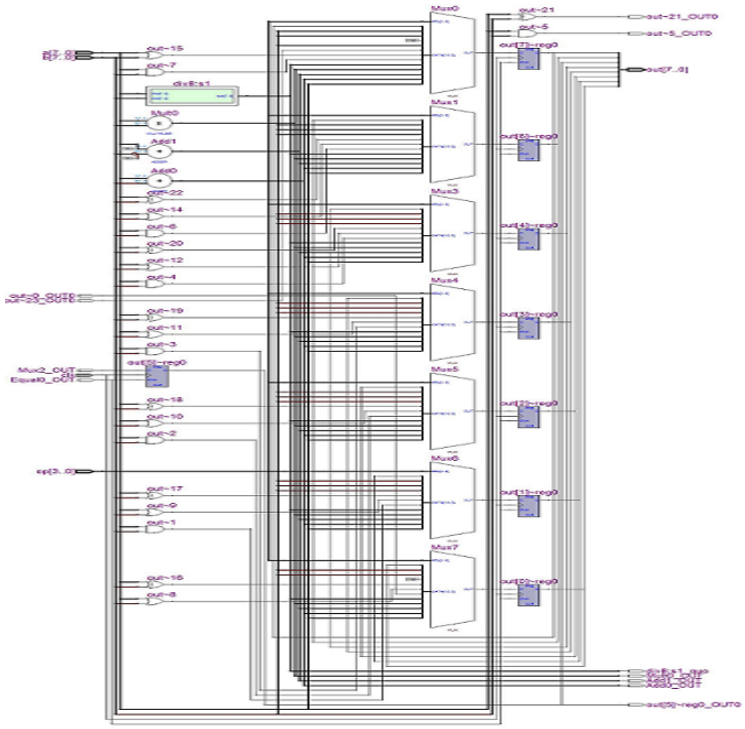

Figure 4. RTL view of ALU

9. SYNHESIS RESULTS

Cryptographic algorithms are implemented on the NIOS II economy based soft core processor using them as the wrapper for testing. The performances of these algorithms on the wrapper are tested with respect to area, speed and logics elements involved. Figure 5 shows the chip planner view for these algorithms which gives the area involved for processing. NIOS II processor results better than other wrappers for testing these algorithms.

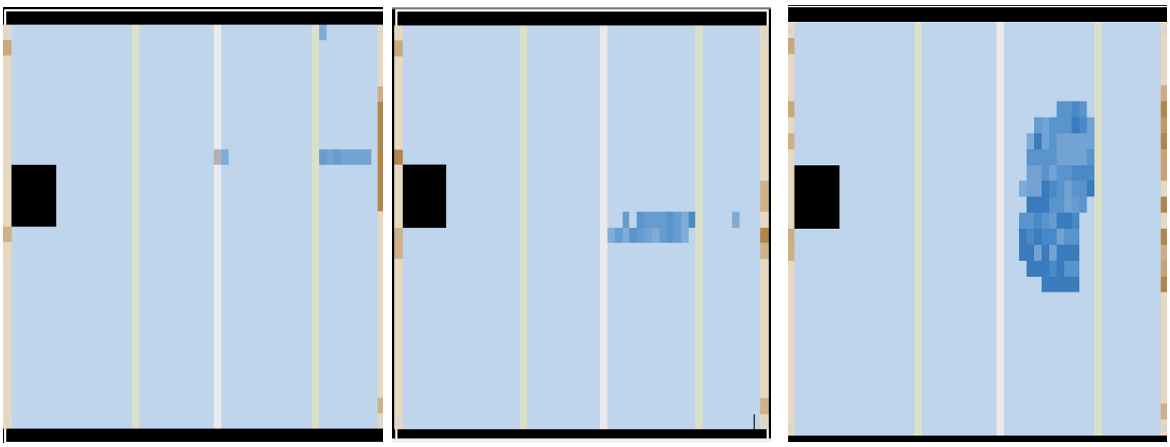

Figure 5. Chip planner view of AES, RC5, SHA algorithms

Table 1 gives the comparison between the various cryptographic algorithms explained in this work in terms of area and memory. The number of registers and the memory determines the processing speed of the

Table 1. Comparison between various cryptographic algorithms

Parameters	AES	RC5	SHA	ALU
Logic elements	4.544	261	1.395	114
Registers	3.968	93	893	0
Memory	704.512	900	0	0
Pins	385	19	74	35

10. CONCLUSION

This paper presents a design and testing of cryptographic algorithms based on NIOS II processor soft core processor. From the above result the test wrapper using NIOS II is performance is better than other wrappers. The cryptographic algorithms are tested over the soft core processor for their performance and results are obtained. Chip planner view shows the area consumed by logic elements for executing the algorithms. NIOS II processor performance is evaluated and results are discussed.

REFERENCES

[1] Jeremy Lee, Mohammad Tehranipoor, Chintan Patel, Jim Plusquellic, Securing Designs against Scan-Based Side-Channel Attacks, *IEEE Transactions on Dependable and Secure Computing*, Vol. 4, No. 4, October-December 2007**.**

[2] Youhua Shi, Nozomu Togawa, Masao Yanagisawa, Tatsuo Ohtsuki, Design for Secure Test - A Case Study on Pipelined Advanced Encryption Standard, *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2007.

[3] B. Yang, K. Wu, and R. Karri, *Secure Scan: A Design-for-Test Architecture for Crypto Chips*, Proceedings ACM/IEEE Design Automation Conference (DAC), June 2005, pp. 135-140.

[4] P. Varma and S. Bhatia, "*A Structured Test Re-Use Methodology for Core-Based System Chips*", in Proc. International Test Conference, 1998, pp. 294–302.

[5] E.J. Marinissen, R. Arendsen, G. Bos, H. Dingemanse, M. Lousbera, and C. Wouters, "*A Structured and Scalable Mechanism for Test Access to Embedded Reusable Cores*", in Proc. International Test Conference, 1998, pp. 284–293.

[6] I. Ghosh, S. Dey, and N.K. Jha, "*A Fast and Low Cost Testing Technique for Core-Based System-on-Chip*", in Proc. Design Automation Conference, 1998, pp. 542–547.

[7] V. Immaneni and S. Raman, "*Direct Access Test Scheme Design of Block and Core Cells for Embedded ASICs*", in Proc. International Test Conference, 1990, pp. 488–492.

[8] P. Varma and S. Bhatia, "*A structured test reuse methodology for corebased system chips*", in Proc. of ITC, pp. 294–302, October 1998.

[9] A. Sehgal and et.al, "*Test cost reduction for SoCs using virtual tams and lagrange multipliers*", in Proc. of DAC, pp. 738–743, June 2003.

[10] T. Waayers, E. J. Marinissen, and M. Lousberg, "*IEEE std 1500 compliant infrastructure for modular SOC testing*", in Proc. of ATS, p. 450, November 2005.

[11] IAIK. SHA-3 hardware implementations. http://ehash.iaik.tugraz.at/wiki/SHA-3 Hardware Implementations.

[12] CERG at George Mason University. Hardware interface of a Secure Hash Algorithm (SHA). Functional Specification, October 2009.