THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

NIOS II Based Secure Test Wrapper Design for Testing Cryptographic Algorithms

K. Chakrapani
Department of Information Technology, SASTRA University, Tamil Nadu, India
Dr. P. Neelamegam
School of Electrical and Electronics Engineering, SASTRA University, Tamil Nadu, India

Abstract:
Cryptographic algorithms require an infrastructural support for testing their efficiency against security attacks. Many methods are available for testing the cryptographic primitives. One of them is to test the algorithms by using cryptographic chips. These chips are not suitable for general purpose algorithms. Though built-in self-tests are applied to test the intellectual properties of these chips, they still suffer from many problems such as side channel attacks, black-holes, high area overhead, and many more. To overcome the above mentioned defects, a test wrapper is designed and tested using NIOS II economy soft core processor. NIOS II soft-core processors perform well for testing the cryptographic algorithms. NIOS II's soft core processor and cryptographic algorithms are utilized for testing and execution. Tests with respects to area optimization, memory and speed are performed and the results are provided.

Keywords: *Cryptographic algorithms, NIOS II, Soft-core processors, Test Wrappers*

1. Introduction

Advancements in networking, have resulted in an increased demand for protection of data and information from spoofing and other attacks. In order to overcome this crisis, various cryptographic algorithms are used for data protection. The cryptographic algorithms are tested on chips for evaluating their performance efficiency, to know whether they fulfill their tasks. These cryptographic algorithms are in general proven mathematical models. 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 has also become a crucial factor. Wrappers are used for testing this IP cores on their feasibility, faults, performance evaluation, etc. Wrappers are a 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 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.

System on chip (SOC) is nothing but a chip which integrates the processors, memory and interface devices in the form of a core IC. Testing these SOCs were a major constrain in 1999, but later many methods [1, 2] are developed for testing IP cores. Test access machine (TAM) and test wrappers were developed 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 turn reduces the memory requirement for the vector in the chip. Wrappers operate at various modes such as normal, core, interconnect and bypass test.

A wrapper called Test collar [3] was developed for testing cores, but the interconnect test is not performed using this wrapper. Balanced wrapper chain is used which consist of cores in chain and has an internal scan which reduces the time taken for scanning [4]. Recently many varieties of wrappers are being developed such as core transparency [5], multiplexed access [6]. All these wrapper-designs solves only a few problems but still have more constrains along with modifications. Various cryptographic algorithms are verified for its performance efficiency by testing them on chips [7, 8]. Various corrections and advancements in algorithms like RC5, Hash, Advanced hashing etc., are achieved by these testing methodologies.

In this paper we have tested the wrapper using NIOS II economy soft core processor for various cryptographic algorithms. The time taken for these algorithms to execute has also been discussed. Wrapper's performance is also analyzed and reported. The work is split up as section 2 providing the functional description of NIOS II processor, section 3 presenting the various cryptographic algorithms and their primitives. In section 4 synthesis results are discussed and finally the conclusion is drawn in section 5.

2. Functional Description

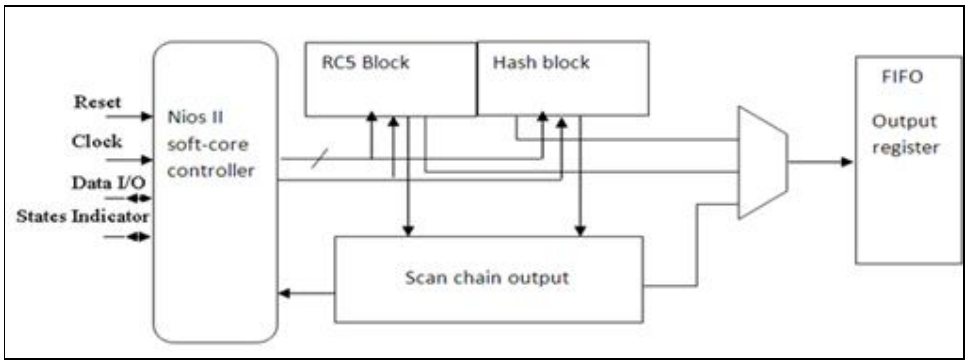


Figure 1: Functional block diagram of NIOS II processor

Fig. 1 describes the functional block diagram of NIOS II soft-core-processor based wrapper design. NIOS II processor is given with control and data as inputs. The RC5 and Hash blocks generate test outputs for the given set of input data. These generated outputs are given to the scan chain output where comparison takes place and its output is given back to the processor for comparing them with the inputs. On the same par, the 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 sequence. 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 there is any change in the hardware model of the proposed system, it can be easily modified by altering a few commands. Modification of the hardware can be easily reflected with NIOS II based soft-core processor. These processors utilize lesser 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.

3. Cryptographic Algorithms

A lot of cryptographic algorithms have been developed for secret data communication for any critical application. 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 message at the receiver side. It is impossible to incorporate different cryptographic algorithms for personal 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, the computational complexity increases.

In this work, algorithms which are proven to be secure in the public scrutiny for a long time has been taken. These algorithms are tested in wrappers based on NIOS II processor. The performance, time taken for execution, efficiency is calculated using the 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.

3.1. AES Encryption

Advanced Key Encryption (AES) is a private key encryption technique used from a long time. This algorithm uses different keys for different block size. Each block in this technique has a length of 128 bit with different key length. It is a symmetric key algorithm which makes use of the same key for the purpose of 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 sub-bytes, shift-row, and mix-columns will take place. This round key process is repeated for many iterations and reverse of same will be the decrypting process. Fig. 2 shows the schematic for AES encryption.

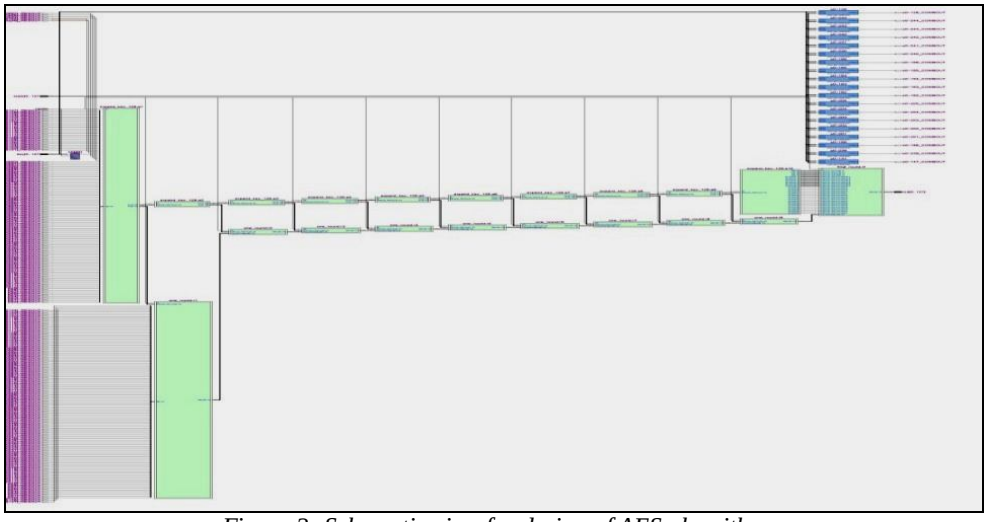


Figure 2: Schematic view for design of AES algorithm

3.2. RC5 Algorithm

RC5 is a block cipher symmetric key encryption which is simpler than the other cryptographic algorithms. This algorithm has blocks of various sizes used according to the application. Number of rounds for encryption also varies from 0 to 255 as per need. 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. The algorithm is a set of data dependent rotations in its encryption and decryption process. 64 bit key is used for encryption in RC5 algorithm. Fig. 3 shows the schematic of RC5 algorithm.

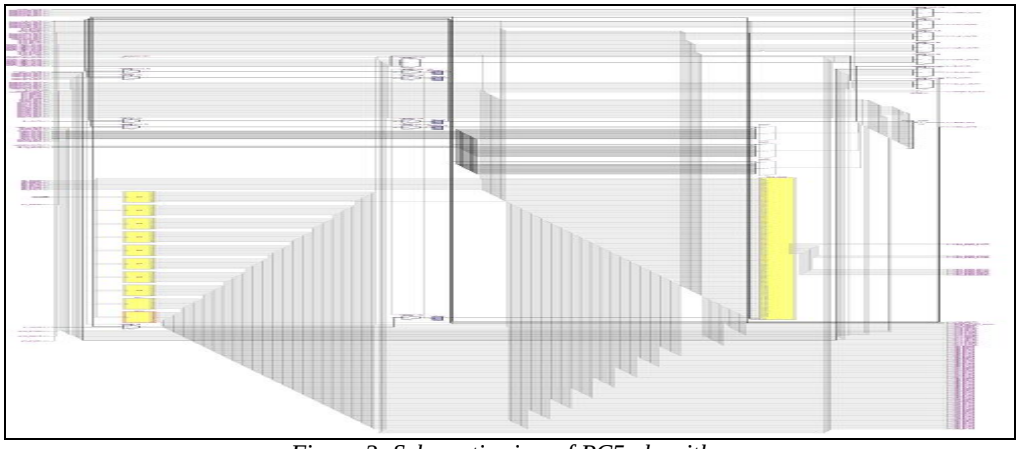


Figure 3: Schematic view of RC5 algorithm

3.3. Hash Algorithm

Secure hash algorithm (SHA) is a cryptographic hash function which is mostly used in case the of integrity check. These cryptographic hash functions are difficult to rebuild or construct again in reverse engineering process thus providing high security for 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. Fig. 4 shows the RTL view of SHA algorithm.

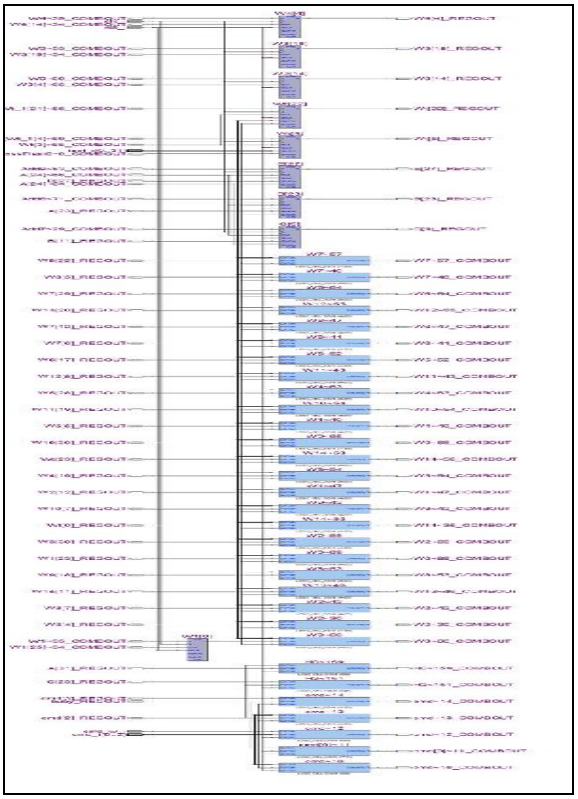


Figure 4: RTL view of HASH Algorithm

3.4. ALU

Arithmetic logic unit, a digital circuit functions to perform all 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 require ALU for numerous logical OR and EXOR operations. Fig. 5 shows the RTL view of ALU.

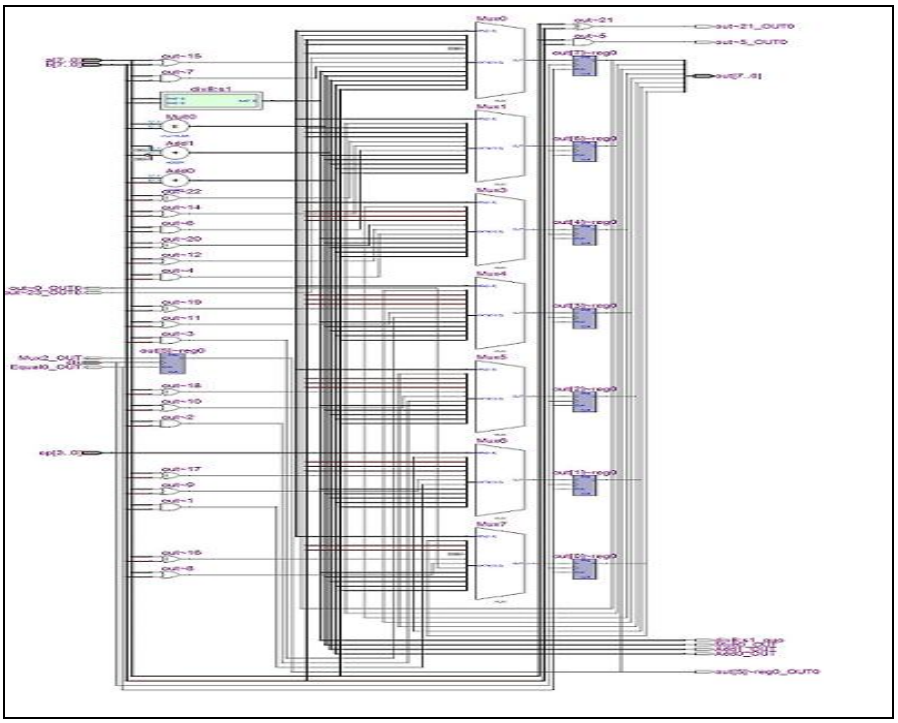
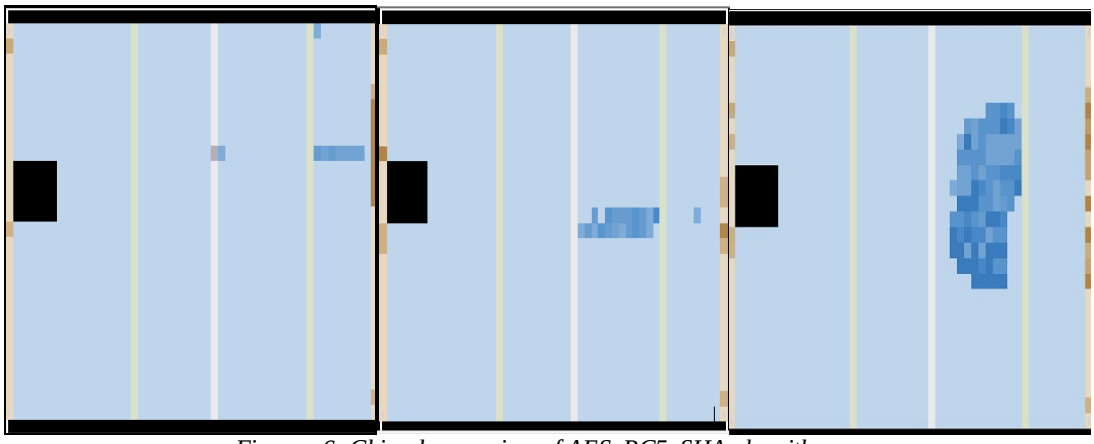


Figure 5: RTL view of ALU

4. Synthesis Results

Cryptographic algorithms are implemented on the NIOS II economy based soft core processor which functions as the wrapper for testing. The performances of these algorithms on the wrapper are tested with respect to area, speed and logics elements involved. Fig. 6 shows the chip planner view for these algorithms which gives the area involved for processing. NIOS II processor based wrapper results are better than other wrappers for testing these algorithms.



Figgure 6: 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 various cryptographic components.

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

Table 1: Comparison between various cryptographic algorithms

5. Conclusion

This paper presents a design and testing of cryptographic algorithms based on NIOS II's soft core processor. From the above results, the developed test wrapper's 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 was evaluated and the results were discussed. Memory required is also less compared to other processors. Area required is optimized using NIOS II processor and it is flexible for design of complex circuits.

6. References

1. A. Sehgal and et.al, "Test cost reduction for SoCs using virtual tams and lagrange multipliers," in Proc. Of DAC, June 2003,738–743.
2. T. Waayers, E. J. Marinissen, and M. Lousberg, "IEEE std 1500 compliant infrastructure for modular SOC testing," in Proc. of ATS, November 2005, 450.
3. P. Varma and S. Bhatia, "A Structured Test Re-Use Methodology for Core-Based System Chips," inProc. International Test Conference, 1998, 294–302.
4. 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, 284–293.
5. 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, 1998,542–547.
6. V. Immaneni and S. Raman, "Direct Access Test Scheme Design of Block and Core Cells for Embedded ASICs," in Proc. International Test Conference, 1990, 488–492.
7. 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.
8. B. Yang, K. Wu, and R. Karri, Secure Scan: A Design-for-Test Architecture for Crypto Chips, in Proc. ACM/IEEE Design Automation Conference (DAC),June 2005, 135-140