IJCAES
ISSN: 2231-4946
Volume III, Special Issue, August 2013

International Journal of Computer Applications in Engineering Sciences
Special Issue on National Conference on Information and Communication (NCIC'13)
www.caesjournals.org

An Efficient Logic Test Structure For Low Power Testing

P.Anand Selvakumar[1] , Mrs.K.L.Hemalatha[2]
ME VLSI DESIGN, Easwari Engineering College, Chennai
anandskp89@gmail.com

***Abstract*- In this paper proposes a new single cycle access test structure for logic test. It will eliminates the unnecessary dynamic power consumption problem of conventional shift-based scan chains during switching transition in the scan FF and also reduces the accessing time into one clock cycles. This leads to more realistic circuit behavior during stuck-at and at-speed tests. It enables the complete test to run at much higher frequencies equal or close to the one in functional mode. It will be shown, within one clock cycle testing can be achieved compared to other published solutions we carried out testing with some published solutions on ISCAS'89 net lists. And finally we developed BIST in steganography design where initially we developed new algorithm with high embedding capacity and also undetectable by statistical analysis methods such as Regular-Singular (RS) and Chi-square analyses. Here we use LFSR as key module to overcome the security holes in the existing systems. In functional mode this LFSR module will be used for steganography application and in testing mode this will act as a random generator .The structure allows an additional on-chip debugging signal visibility for each register.**

***Keywords*- LSB steganography, Built-in self-test (BIST), linear feedback shift register (LFSR).**

I. INTRODUCTION

In recent years, the design for low power has become one of the greatest challenges in high-performance very large scale integration (VLSI) design. As a consequence, many techniques have been introduced to minimize the power consumption of new VLSI systems. However, most of these methods focus on the power consumption during normal mode operation, while test mode operation has not normally been a predominant concern. However, it has been found that the power consumed during test mode operation is often much higher than during normal mode operation.

Another category of techniques used to reduce the power consumption in scan-based built-in self-tests (BISTs) is by using scan chain-ordering techniques [7]. These techniques aim to reduce the average-power consumption when scanning in test vectors and scanning out captured responses. Although these algorithms aim to reduce average-power consumption, they can reduce the peak power that may occur in the CUT during the scanning cycles, but not the capture power that may result during the test cycle (i.e., between launch and capture).

Automatic test pattern generation (ATPG) for sequential VLSI circuits is an NP-complete problem with an exponential complexity. The complexity of combinatorial logic changes. Less complex logic is tested within a few capture cycles, generating an immense number of don't cares during the rest of the test, even when test compression methods are used. Complex and hard to test logic needs to be stimulated and captured quite often but the pattern need to be shifted throughout the complete scan chain. One approach to reduce test time is to use parallel scan chain. This led to a massive increase of parallel scan chains to drive down the length of the scan chains. To further reduce test data volume, a built-in-self-test (BIST) mechanism is used.

Mostly LFSR is used as random number generator to give random inputs for testing. So for any BIST application LFSR will be main design module.

II. PSEUDO-RANDOM NUMBER GENERATOR

Pseudo random number generator (PRNG) prevents invaders to find message bits easily. A secret key can be used as a seed for PRNGs. Using a seed causes PRNGs to generate the same random numbers on receiver side as on the sender side. In this paper, a linear feedback shift register (LFSR) is used as PRNG.

A. Implementation of LFSR

A LFSR is made of sequential shift-register with combinational feedback logic connected to it which can generate a sequence of binary values in a pseudo-random manner. A design modeled around LFSRs often has both speed and area advantages over a functionally equivalent design that does not use LFSRs.

Feedbacks around an LFSR's shift register are connected to the certain points (taps) of LFSR construction and constitute either XORing or XNORing these taps to provide taps back into the register.

The selection of taps determines how many values can be generated in a given sequence before the sequence is repeated. Certain tap arrangement lead to maximal length sequences of (2n - 1).

B. *Single Cycle Access Structure*

The key element of the single cycle access structure with hold mode (SCAhS) is the signal cycle access register (Flip-Flop, FF) with hold mode (SCAh-FF). It is based on a standard scan register (S-FF) and uses two more 2-to-1 multiplexers. The new SCAh-FF can be seen in Fig. 1. The SCAh-FF has one more input and one more output compared to the standard shift register (S-FF). The inputs clock {clk}, data-in {di}, and scan-in {si} still exists. The scan-enable is now a 2 bit bus {se[0:1]}. An additional scan output pin {so} is added. The reset input and inverse output pins are not shown. The internal logic enables the register to run in one additional hold mode, whereas the additional output multiplexer can bypass the register to directly drive the value of {si}.

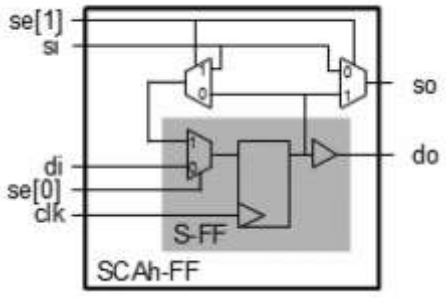

Fig 1.SCA FF with hold mode

Truth table I
TRUTH TABLE OF SCAh-FF

se[0:1]	do @ clk	so	mode
00	di	si	functional
01	di	do	async. read
10	do, unchanged	si	hold
11	Si	do	sync. write/read

In order to reduce the area overhead of a SCAhS, a simpler SCA-FF is discussed. It adds only one 2-to-1 MUX to the standard S-FF The truth table is shown in Table I. It only has one {se} input, which is connected to the individual line-select signal. The pin connected to the global enable signal in the SCAhS is removed, so that the complete global scan enable tree becomes obsolete. The SCA-structure (SCAS) connectivity and page organization equals the one of the SCAhS without the global scan enable {gse}.

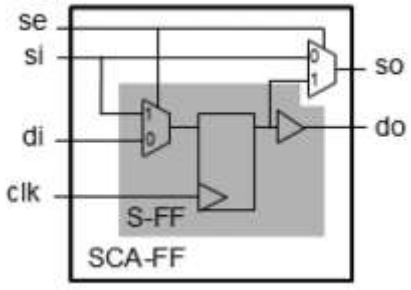

Fig 2.SCA FF without hold mode

the gated SCAS (gSCAS), which has all the benefits of the SCAhS but only has the area overhead of the SCAS. The hold function of the SCAh-FF is missing in the SCA-FF. It is instead built into the gated clock tree of the gSCAS The scan path reaches from the scan-in AND-selector over the SCA-FF chain (by connecting the scan-out pins of each SCA-FF with the scan-in pins of the succeeding SCA-FF) and is connected with the input of the XOR-tree. The individual line-select signals {ls} are connected with the {se} input of the SCA-FF in the relevant line. All SCA-FF on a line are clocked by a gated clock element (gcl). The gcl is driven by the clock and the line-select signal. The gated clock element can be enhanced, if a clock enable signal {ce} generated by combinatorial logic exists. The global scan enable signal is connected with each gcl, which is already the case in SS if gated clock elements are used to propagate the clock during shift.

At circuit level, this strategy is applied by the so-called "gated clock" approach which disables the clock of FFs More specifically, for FFs(flipflop) without an enable signal,we can adopt the strategy proposed in [5] and modified in [6], [7] as it is shown in Fig. 2. This is done by activating the FF only when the input signal is different from the actual output value. As itvcan be easily understood, this approach is perfectly compatible with a LFSR only adding some extra gates. It is worth noting that the XOR and the NAND gates used to implement the gating can be implemented as a single gate (from hereinafter called XORNAND gate) as shown in Fig. 2. This is due to the complementary output always available in every FF.

To analytically evaluate the power consumption of the gated clock approach applied to a LFSR, we have to take into account also the dissipation introduced by the extra gates that are employed to implement the gated clock circuits, as well as the load effects introduced by these gates with respect to the traditional one.

Truth table II
TRUTH TABLE OF SCA-FF

gse	ls	ce	gclk	mode
0	X	0	0	functional disabled
0	X	1	propagate clk	functional enabled
1	0	X	0	hold mode
1	1	X	propagate clk	write mode

In order to evaluate the power reduction obtained by applying the gated-clock approach to a SCA without hold FF, we have to analytically compare relationships (2) with (6). As preliminary results, we obtained that.

$$C_{CK} > \frac{\alpha}{1-\alpha}\left(C_{inFF\_CK} + C_{XORNAND} + 4C_{inXORNAND} + \frac{C_{INV} + C_{inINV}}{n}\right)$$

which defines the technological condition (and the circuital so lutions for the gate's implementation) so that the gate-clock approach leads to an improvement in terms of power reduction compared to the traditional S-FF and both SCA-FF implementation.

III. STEGANOGRAPHY

In the modern world, information is converted from paper type to digital information. Therefore, security improvement in data saving and exchanging is important. Different techniques of cryptography are used for data encryption but all of these methods can be recognized by invaders. If the information can be embedded in a medium in such a way that it cannot be observable easily, it will not raise the suspicion of invaders. This is the main idea of steganography.

The image formats used typically in such steganographical methods are lossless and the data can be directly manipulated and recovered. Since bmp images use lossless compression, one form of LSB attempts to use bmp images. However, other image formats are used as cover image as well.

A. Data hiding process:

Consider S = < x0, x1, … , xn > be the set of pixels of an image which is selected by a pseudo-random number generator. Pseudo random number generator produces random numbers according to the value of seed (stego-key). *x* is the gray value of each pixel. *n* is determined by the size of embedded message and the number of LSB bits in each pixel which can be used to embed messages. It could be calculated by:

$$n = \frac{k}{m}$$

Where *k* is the length of bit stream of embedded message, and *m* is the number of bits used to embed messages in each pixel.

B. Message Bit Randomizer Module

This part of design changes message bits so that if invaders find them, they cannot construct the message without access to secret key and the LFSR architecture. In each clock cycle, message bits must be XORed by a random number. The result of XOR operation will be embedded in pixels. At receiver side, extracted LSBs of each pixel must be XORed with the same random bits to construct the message bits.

A novel combinational randomizer is used for this reason. Figure 2 shows the architecture of this design. Message bits are embedded in least significant bits of a pixel. A 16-bit LFSR with a seed (*seed2* input) generates random values. As shown in Figure 2, for one, two, three and four message bit insertion, four outputs (*y1, y2, y3, y4*) are considered. Input *m* value is changed from one to four by user selection and each value of *m* creates one of the outputs.

Module SHIFT16 contains a 16-bit LFSR that randomly generates sixteen bits in each clock cycle. However, these random values will not be XORed with message bits directly. Random bits from SHIFT16 module will be inserted in another module.

This module contains several multiplexers and LFSRs. In this module, if m=1, sixteen bits insert a 16 to 1 multiplexer. Selector of this multiplexer is connected to a 4-bit LFSR. Therefore, multiplexer selects one of these sixteen inputs as output, randomly. The output will be XORed by one message bit. This process is repeated for every

bit insertion. Figure 3, shows top level view of steg module which contains LFSR and multiplexer for one bit insertion.

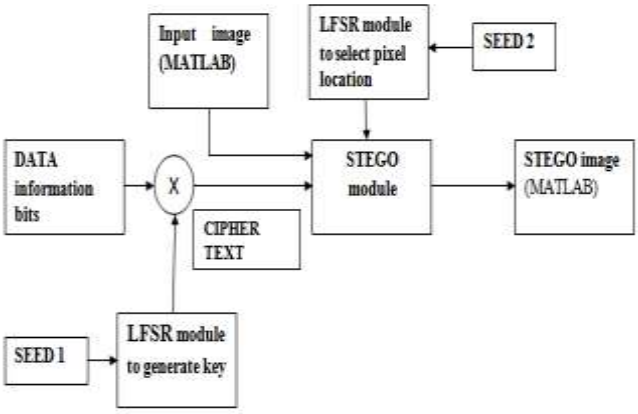

Fig 3. Block diagram of proposed steganography method in functional mode.

IV. PERFORMANCE ANALYSIS

SCAVsSCAgatedFF

Page setup parameter	SCA without hold	SCA with gated clock
Logical elements used	68 (combinational logic unit) ---48(registers)	90(combinational logic unit) ---71(registers)
Total power(mW)	98.66	86.11

SCAh FF Vs SCA FF

Page setup parameter	SCA with hold FF	SCA without hold FF
Area(Logical elements used)	3(combinational logic unit) ---1(registers)	2(combinational logic unit) ---1(registers)
Total power consumes(mW)(static alone)	64.71	64.62

SCA page Vs gSCA page

Page setup parameter	SCA without hold	SCA with gated clock
Area(Logical elements used)	68 (combinational logic unit) ---48(registers)	90(combinational logic unit) ---71(registers)
Total power consumes(mW)	98.66	86.11

Area will be increased considerably in case of Global SCA as compared to SCA without hold page due to AND gates usage in the design. But overall power dissipation will be reduced due to gated clock used in the whole page set up.

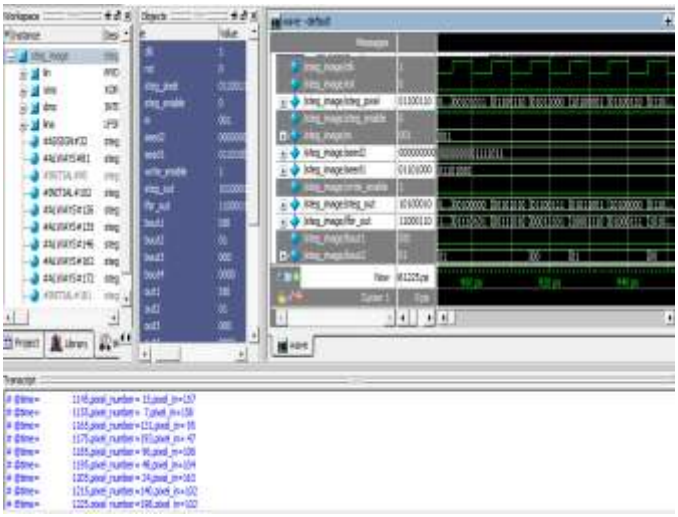

Fig 4. Simulated output

V. CONCLUSION

A single cycle access structure is discussed. Various implementations with and without hold mode as well as gated and partial implementation methods are presented. The aspects peak power consumption, switching activity during test, area, power testing are compared. A guide is given how to select the best implementation. The best solution (gSCAS) is compared to RAS implementations and is superior to all known RAS solutions. If BIST is preferable due to limited chip IOs or partial scan implementation, an address controlled BIST is discussed. The ATPG algorithms can be enhanced with the same methods SS implementations are optimized.

Future work is related to algorithms for reducing the test cycles per net itself, register reordering, pattern optimization for activity reduction and de-compression methods for BIST using the gSCAS.The ISCAS'89 net-lists circuits are tested by using the new single cycle access test structure for logic test. All three types of Flip-flops are tested (SCA with hold, SCA without hold and gated clock based SCA). With these methods the BIST (Build in self test) application is achieved with minimum power and high speed access (single cycle access) of individual elements in the design. Finally the proposed method is proved for testing is more efficient as compared to standard scan based shift scan method in terms of power and speed.

REFERENCES

[1] A. P. Chandrakasan, N. Verma, and D. C. Daly, "Ultra low power electronics for biomedical applications," *Annual Review of Biomedical Engineering*, vol. 10, pp. 247-274, August 2008.

[2] L. Mateu and F. Moll, "Review of energy harvesting techniques and applications for microelectronics," *Proc. SPIE Microtechnologies for the New Millennium*, pp. 359-373, 2005.

[3] V. Raghunathan and P. H. Chou, "Design and power management of energy harvesting embed ed systems," *Proc. International Symposium on Low Power Electronics and Design*, pp. 369-374, 2006.

[4] C. Lu, S. P. Park, V. Raghunathan, and K. Roy, "Efficient power conversion for ultra low voltage micro scale energy transducers," *Proc. Design, Automation and Test in Europe*, pp. 1602-1607, 2010.

[5] Optobionics Corp. (http://optobionics.com/)

[6] C. Lu, V. Raghunathan, and K. Roy, "Maximum power point considerations for micro-scale solar energy harvesting systems," *Proc. International Symposium on Circuits and Systems*, pp. 273-276,2010.

[7] E. Esram and P. L. Chapman, "Comparison of photovoltaic array maximum power point tracking techniques," *IEEE Transactions on Energy Conversion*, vol. 22, no. 2, pp. 439-449, June 2007