IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Physical Unclonable Functions Based Random Number Generators using Built-In-Self-Test

M.V.ASHOK KUMAR M.TECH, T.RAGHUVARAN M.TECH Department of Electronics and Communication Engineering

Sir C Ramalinga Reddy Polytechnic, Eluru, Andhra Pradesh, India

Abstract

The Internet of Things (IoT) is a fast evolving paradigm where remotely identifiable physical objects form an active network, and are able to operate independently without external control. With these smart devices automatically connecting to each other and exchanging private and sensitive data, the potential for malicious attacks greatly increases. As a result, it is widely accepted that the most challenging aspect of IoT will be to ensure security and privacy. This paper proposes an important cryptographic primitive i.e. transition controlled random number generator, that shares overlapping properties and often have structural similarities with PUFs. The integrity of any secure system depends largely on the proper functioning of these units. True Random numbers are needed for encryption keys, nonces, padding bits and many more applications. Software approaches to generate random numbers, called Pseudo Random Number Generators (PRNG) are widely adopted and are suitable for most applications. However, they are susceptible to attacks as their outputs are deterministic functions of the seed, which carries all its entropy. Therefore, hardware-based mechanism to extract randomness from physical phenomena is required for cryptographic applications. As data privacy is one of the key requirements of IoT framework, it can benefit from high entropy TRNGs generating secure keys.

1. Introduction

One of the primary properties of any IoT device is a _unique identifier‘. A compact embedded identifier with a small footprint and energy budget is ideal for IoT as a large number of devices will operate in passive mode with limited source of power. Therefore, hardware- based security is well suited for IoT protocols and algorithms. They are also naturally more resistant to physical and side-channel attacks. These facts make Physical Unclonable Functions (PUF) a promising enabler for generation of inherent and indelible device identifiers for IoT security solutions.

PUF is a (partially) disordered physical system: when interrogated by a challenge (or input, stimulus), it generates a unique device response (or output). The response depends on the incident challenge, specific physical disorder and PUF structure. It is common to call an input and its corresponding output a challenge- response pair (CRP). PUFs have been established as an efficient embedded identification primitive over the last decade. Identifying and authenticating individual entities among a large variety of physical devices as demanded by IoT protocol is a challenge. Classic identification methods including serial numbers onchip/ package and ID storage in non-volatile memory are subject to attacks such as removal and remarking. Unclonable marking on the device ICs is important in that it can enable a low overhead identification, fingerprinting, and authentication for a wide range of disparate devices.

However, environmental factors, aging, or attacks from the adversary may deteriorate PUF performance and thereby cause delays, and more importantly, security threats. Therefore, they cannot guarantee a fully standalone solution as the root-of-trust of IoT entities without a careful analysis. As shown several times in practice, when the random PUF response values are not exactly random, catastrophic security failures occur. For example, several analysis and attacks on PUF have highlighted the need for appending

input or output transformations for safeguarding purposes. Moreover as devices connect and share automatically in IoT, stability of the response over a wide range of operational conditions is essential to ensure seamless operation.

2. Existing System

This existing method introduces the methodology for online hardware-based assessment of the robust generation of streams of truly random (unpredictable) PUF responses that are unique to each device. Two main characteristics of PUF are evaluated by the Built-In-Self-Test (BIST) scheme: stability and unpredictability. These evaluations can reveal the operational, structural, and environmental fluctuations in the PUF behavior that may be caused by variations, aging, or attacks. The continuous and online monitoring of PUF characteristics yields several advantages including: (i) detection of changes/attacks during the PUF operation, (ii) providing an on-the-fly measure of confidence on the randomness/ robustness of the CRPs, (iii) ensuring PUF stability by validating CRPs before adding them to library, (iv) reporting the exact conditions in the local PUF test site for a more granular debugging, and (v) enabling active adjustment and improvements of the PUF operations.

Since unpredictability is an important property for both TRNGs and PUFs, the resource usage is designed by a BIST scheme that shares resources. Besides these, they have include tests for internal structure or TRNGs. A fall in entropy level in any of the units is an indicator of an active attack or imminent failure of the TRNG. PUF cannot be modeled as a deterministic process. Standard randomness test suite is used to evaluate the unpredictability of PUF response. Fixed width TRNG‘S were used leading to high memory in-efficiency. This circuit leads to overall worst case system latency. The circuit that is being tested is called the *circuit-under-test (CUT)*. The block diagram of the system is shown in Fig.1. There is a *test pattern generator* which applies test patterns to the CUT and an *output response analyzer* which checks the outputs. The test pattern generator must generate a set of test patterns that provides high fault coverage in order to thoroughly test the CUT. Pseudo-random testing is an attractive approach for BIST. A linear feedback shift register (LFSR) can be used to apply pseudo-random patterns to the CUT. An LFSR has a simple structure requiring small area overhead. Moreover, an LFSR can also be used as an output response analyzer thereby serving a dual purpose. BIST techniques such as circular BIST [Stroud¬88], [Krasniewski¬89], and BILBO registers [Koenemann 79] make use of this advantage to reduce overhead.

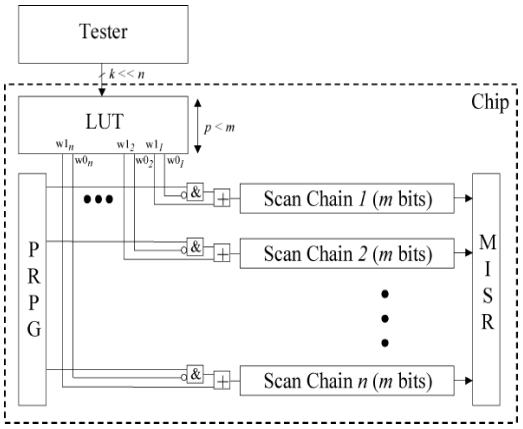

Fig.1Block Diagram for BIST

There are limits on the *test length*, which is the number of pseudo-random patterns that can be applied during BIST. One limit is simply the amount of time that is required to apply the patterns. Another limit is the fault simulation time required to determine the fault coverage. A third limit is heat dissipation for an unpackaged die. Thus, in order for pseudo-random pattern testing to be effective, a high fault coverage must be obtained for an ―acceptable‖ test length. What is considered acceptable depends on the particular test environment.

3.Proposed System : In this paper, we propose a PRPG for LP BIST applications. The generator primarily aims at reducing the switching activity during scan loading due to its preselected toggling (PRESTO) levels**.**

1) *Minimum transitions:* In the proposed pattern, each generated vector applied to each PRNG output, which can minimize the input transition and reduce test power.

2) *Uniqueness of patterns:* The proposed sequence does not contain any repeated patterns, and the number of distinct patterns in a sequence can meet the requirement of the target fault coverage for the CUT.

3) *Uniform distribution of patterns:* The conventional algorithms of modifying the test vectors generated by the LFSR use extra hardware to get more correlated test vectors with a low number of transitions. However, they may reduce the randomness in the patterns, which may result in lower fault coverage and higher test time.

4) *Low hardware overhead consumed by extra TPGs:* The linear relations are selected with consecutive vectors or within a pattern, which has the benefit of generating a sequence with a sequential de-compressor. Hence, the proposed TPG can be easily implemented by hardware

B. Transition Controlled PRNG

In Fig. 2 the basic structure of a PRNG generator is shown. An n-bit PRPG connected with a phase shifter feeding scan chains forms a kernel of the generator producing the actual pseudorandom test patterns. A linear feedback shift register or a ring generator can implement a PRPG. More importantly, however, n hold latches are placed between the PRPG and the phase shifter. Each hold latch is individually controlled via a corresponding stage of an n-bit toggle control register. As long as its enable input is asserted, the given latch is transparent for data going from the PRPG to the phase shifter, and it is said to be in the toggle mode. When the latch is disabled, it captures and saves, for a number of clock cycles, the corresponding bit of PRPG, thus feeding the phase shifter (and possibly some scan chains) with a constant value. It is now in the hold mode. It is worth

A) BIST Application : noting that each phase shifter output is obtained by XOR-ing outputs of three different hold latches. Therefore, every scan chain remains in a low-power mode provided only disabled hold latches drive the corresponding phase shifter output.

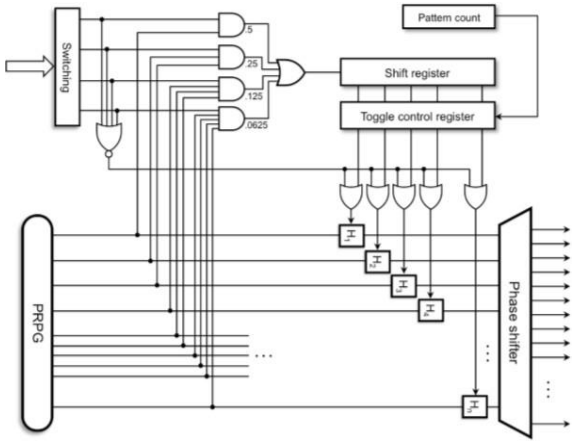

Fig.2. Basic architecture of Transition PRN generator.

C. Hold and Toggle registers

Two additional parameters kept in 4-bit Hold and Toggle registers determine how long the entire generator remains either in the hold mode or in the toggle mode, respectively. To terminate either mode, a 1 must occur on the T flip-flop input. This weighted pseudorandom signal is produced in a manner similar to that of weighted logic used to feed the shift register. The T flip-flop controls also four 2-input multiplexers routing data from the Toggle and Hold registers.

It allows selecting a source of control data that will be used in the next cycle to possibly change the operational mode of the generator. For example, when in the toggle mode, the input multiplexers observe the Toggle register. Once the weighted logic outputs 1, the flip-flop toggles, and as a result all hold latches freeze in the last recorded state. They will remain in this state until another 1 occurs on the weighted logic output. The random occurrence of this event is now related to the content of the Hold register, which determines when to terminate the hold mode.

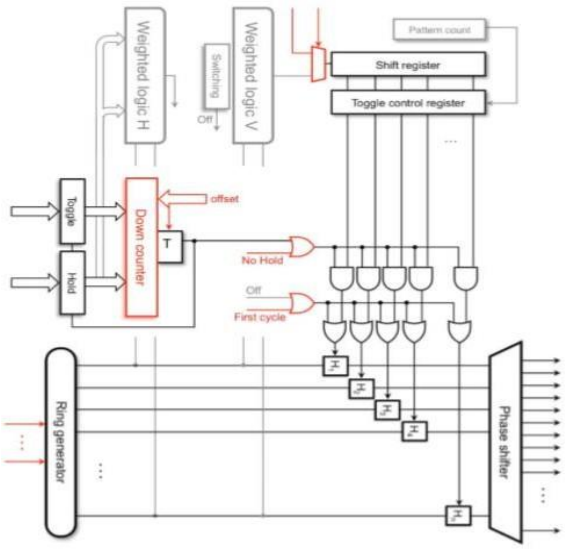

Fig 3 LP De-Compressor

1. System Architecture & Module Description

LP-Decompressor

In order to facilitate test data decompression while preserving its original functionality, the circuitry of Fig.2 has to be modified. This is shown in Fig. 3. The core principle of the de-compressor is to disable both weighted logic blocks (*V* and *H*) and to spread out deterministic control data and to facilitate test data decompression. A multiplexer placed in front of the shift register select the content of the toggle and control register. The Toggle and Hold registers are employed to alternately preset a 4-bit binary down counter, and to determine durations of the toggle and hold phases. When this circuit reaches the zero value, it causes a dedicated signal to go high to toggle the T flip-flop. The same signal allows the counter to have the input data kept in the Toggle or Hold register entered as the next state.

Both the T flip-flop and the down counter need to be initialized for every test pattern. The initial value of the T flip flop decides whether the decompressor will begin to operate either in the hold mode or in the toggle mode, while the initial value of the counter, determines that mode‘s duration. As can be seen, functionality of the T flip-flops remains the same as that of the LP PRPG but two cases. First, the encoding procedure may completely disable the hold phase by loading the Hold register with an appropriate code, for example, 0000. If detected that there is no Hold signal, it overrides the output of the T flip-flop by using an additional OR gate. Therefore, the entire test pattern is going to be encoded within the toggle mode exclusively. In addition, all hold latches have to be properly initialized. Hence, a control signal First cycle produced at the end of the ring generators initialization phase reload all latches with the current content of this part of the decompressor. Finally, external ATE channels which feeding the original PRPG allows to implement a continuous flow of test data decompression such as the dynamic LFSR reseeding. Given the size of PRPG, the number of scan chains and the corresponding phase shifter, the switching code, the offset, as well as the values kept in the Toggle and Hold registers, the entire decompressor will produce the decompressed test patterns having a desired level of toggling provided the scan chains are balanced. The corresponding encoding procedure, including an appropriate selection of the aforementioned parameters contains several steps.

Encoding Procedure

The input signal allows the counter to have the input data kept in the Toggle or Hold register entered as the next state. Both the down counter and the T flip-flop need to be initialized every test pattern. The initial value of the T flipflop decides whether the decompressor will begin to operate either in the toggle or in the hold mode, while the initial value of the counter, further referred to as an offset, determines that mode‘s duration.

First of all, the encoding procedure may completely disable the hold phase (when all hold latches are blocked) by loading the Hold register with an appropriate code, for example, 0000. If detected (No Hold signal in the figure), it overrides the output of the T flip-flop by using an additional OR gate, as shown in Fig.3 As a result, the entire test pattern is going to be

encoded within the toggle mode exclusively. In addition, all hold latches have to be properly initialized.

The actual toggle rate (TR) percentage, measured as a weighted transition metric, is given by

$$TR = 50(n/S)(T/(T + H))$$

where n is the number of scan chains, S is the total number of scan chains, and T and H are the durations of toggle and hold periods, respectively. The actual algorithm to yield the desired values of T, H, and O can be summarized as follows,

1) Given a test cube and its transitions, find the earliest transition ending point e and assign a single bit toggle phase ($T = 1$) to cycle e.

2) Mark all transitions crossing e, as they will not end up within a single hold period.

3) Increase the toggle period by extending it up to the next unmarked transition starting point. Repeat this step as long as the duration of the toggle period does not exceed a certain threshold (in this paper, ten cycles).

4) Find the next unmarked transition ending point e‘—it determines a duration H of the hold period unless H is larger than a certain threshold. In the former case go to step 6, otherwise invoke step 5.

5) Find the value of H that minimizes the ratio T/H and, by adding new hold and toggle phases, keeps the cycle e_ within a toggle period.

6) Set the offset period O to e mod $(T + H)−H$, if we begin with an incomplete toggle period, and $O = e$mod $(T + H)$, otherwise.

7) Adjust the values of H, T, and O if some of the remaining unmarked transitions lie entirely within a single hold period. Ensure that the sum $T + H$ remains unchanged. The ratio T/H, on the other hand, may vary, thus its minimizing can guide this step toward an optimal solution.

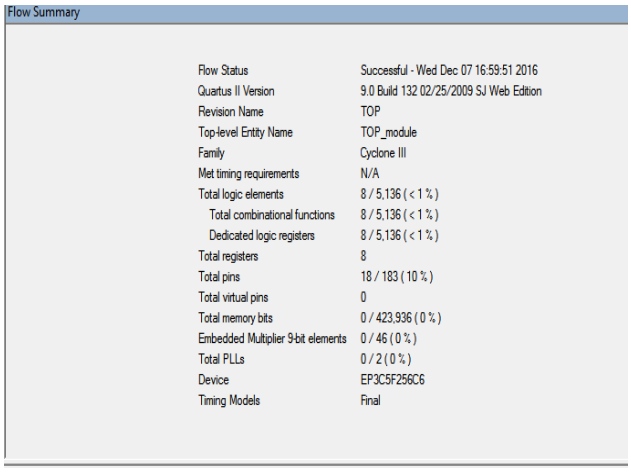

Fig.4 Flow Summary Report

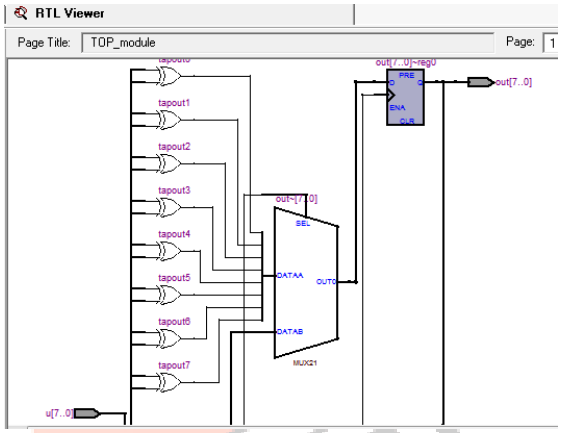

Fig. 5 RTL View of Random Number Generator

CONCLUSION

In this paper, we proved the low complexity and high-performance of proposed transition controlled PRNG and the LP decompresser design and its testing quality metrics. The switching activity can be easily control the generator, so that the resultant test vectors can either yield a desired fault coverage faster than the conventional pseudorandom patterns while still reducing toggling rates down to desired levels, and offer visibly higher coverage numbers if run for comparable test times. And this design is extended into fully functional test data decompressor with the ability to control scan shift-in switching activity through the process of encoding. The efficiency of proposed combine test compression with logic BIST is verified and proved to deliver high quality test.

REFERENCES

[1] Y. Zorian, ―A distributed BIST control scheme for complex VLSI devices,‖ in *11th Annu. IEEE VLSI Test Symp. Dig. Papers*, Apr. 1993, pp. 4–9.

[2] P. Girard, ―Survey of low-power testing of VLSI circuits,‖ *IEEE Design Test Comput.*, vol. 19, no. 3, pp. 80–90, May–Jun. 2002.

[3] A. Abu-Issa and S. Quigley, ―Bit-swapping LFSR and scan-chain ordering: A novel technique for peak- and average-power reduction in scan-based BIST,‖ *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 28, no. 5, pp. 755–759, May 2009.

[4] P. Girard, L. Guiller, C. Landrault, S. Pravossoudovitch, J. Figueras, S. Manich, P. Teixeira, and M. Santos, ―Low-energy BIST design: Impact of the LFSR TPG parameters on the weighted switching activity,‖ in *Proc. IEEE Int. Symp. Circuits Syst.*, vol. 1. Jul. 1999, pp. 110–113.

[5] S. Wang and S. Gupta, ―DS-LFSR: A BIST TPG for low switching activity,‖ *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 21, no. 7, pp. 842–851, Jul. 2002.

[6] F. Corno, M. Rebaudengo, M. Reorda, G. Squillero, and M. Violante, ―Low power BIST via non-linear hybrid cellular automata,‖ in *Proc. 18th IEEE VLSI Test Symp.*, Apr.–May 2000, pp. 29–34.

[7] P. Girard, L. Guiller, C. Landrault, S. Pravossoudovitch, and H. Wunderlich, ―A modified clock scheme for a low power BIST test pattern generator,‖ in *Proc. 19th IEEE VTS VLSI Test Symp.*, Mar.–Apr. 2001, pp. 306–311.

[8] D. Gizopoulos, N. Krantitis, A. Paschalis, M. Psarakis, and Y. Zorian, ―Low power/energy BIST scheme for datapaths,‖ in *Proc. 18th IEEE VLSI Test Symp.*, Apr.–May 2000, pp. 23–28.

[9] Y. Bonhomme, P. Girard, L. Guiller, C. Landrault, and S. Pravossoudovitch, ―A gated clock scheme for low power scan testing of logic ICs or embedded cores,‖ in *Proc. 10th Asian Test Symp.*, Nov. 2001, pp. 253–258.

[10] C. Laoudias and D. Nikolos, ―A new test pattern generator for high defect coverage in a BIST environment,‖ in *Proc. 14th ACM Great Lakes Symp. VLSI*, Apr. 2004, pp. 417–420.

[11] S. Bhunia, H. Mahmoodi, D. Ghosh, S. Mukhopadhyay, and K. Roy, ―Low-power scan design using first-level supply gating,‖ *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 3, pp. 384–395, Mar. 2005.

[12] x. Kavousianos, d. Bakalis, and d. Nikolos, ―efficient partial scan cell Gating for low-power scan-based testing,‖ *acm trans. Design autom. Electron. Syst.*, vol. 14, no. 2, pp. 28-1–28-15, mar. 2009.

[13] p. Girard, l. Guiller, c. Landrault, and s. Pravossoudovitch, ―a test Vector inhibiting technique for low energy bist design,‖ in *proc. 17th Ieee vlsi test symp.*, apr. 1999, pp. 407–412.

[14] s. Manich, a. Gabarro, m. Lopez, j. Figueras, p. Girard, l. Guiller, C. Landrault, s. Pravossoudovitch, p. Teixeira, and m. Santos, ―low Power bist by filtering non-detecting vectors,‖ *j. Electron. Test.-theory Appl.*, vol. 16, no. 3, pp. 193–202, jun. 2000.

[15] f. Corno, m. Rebaudengo, m. Reorda, and m. Violante, ‖a new bist Architecture for low power circuits,‖ in *proc. Eur. Test workshop*, may 1999, pp. 160–164.

[16] s. Gerstendorfer and h.-j. Wunderlich, ―minimized power consumption For scan-based bist,‖ in *proc. Int. Test conf.*, sep. 1999, pp. 77–84.

[17] a. Hertwing and h. Wunderlich, ‖low power serial built-in self-test,‖ In *proc. Eur. Test workshop*, 1998, pp. 49–53.