International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 27th Oct 2017. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-9

Title: **AN RELIABLE HIGH SPEED TECHNIQUE FOR RO PUF WITH IMPROVED THERMAL STABILITY FOR LIGHT WEIGHT APPLICATIONS**

Volume 06, Issue 09, Pages: 304 – 310.
Paper Authors

BHARGAVI, V.SABITHA
VAAGDEVI COLLEGE OF ENGINEERING.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

AN RELIABLE HIGH SPEED TECHNIQUE FOR RO PUF WITH IMPROVED THERMAL STABILITY FOR LIGHT WEIGHT APPLICATIONS

[1]BHARGAVI , [2]V.SABITHA

[1]M.Tech Scahloar, Dept of E.C.E, Vaagdevi College Of Engineering

[2]Assistant Professor , Dept of E.C.E, Vaagdevi College Of Engineering

ABSTRACT: Ring oscillators (ROs) based physically unclonable functions (PUFs) are a popular primitive in hardware security. A new technique is to improve the thermal stability with respect to temperature of PUF using ring oscillator. FPGAs are biased under slower or faster frequencies in non-uniform ways depending on the different design of FPGA's programming; even though the pair of ring oscillators are placed and routed equally. A narrative design subtracting the mean frequency of each RO pair derived using only a small training set of devices. Antifuse algorithm for RO-PUF Architecture to reduce the power consumption. This paper concentrates on the delay and power consumption respectively 10ps and 52mW. The results show that the frequency of hybrid RO is least susceptible to temperature over a range is 27◦C.

KEYWORDS: Physical unclonable function, Ring Oscillator, Bi-Directional counter, Temperature stability.

I. INTRODUCTION

Physical Unclonable Functions (PUF) is a creative circuit primitive that extract secret key from physical characteristics of integrated circuits. Initially, Ring oscillator based physical unclonable function is resilient against noise limitations but its response is much adaptable to temperature variations [1]. RO-PUF is superior to other siliconbased PUFs. The unconstructive temperature coefficient of the low-power sub threshold operation of current starved inverters is oppressed to split the variations of differential RO frequencies with temperature changes. Later, a new framework to generate secure PUF authenticates from ring oscillator (RO) PUF with improved hardware efficiency. Controller is used to generate the control signal which controls the stressed RO and reference RO. Antifusing Algorithm is used to reduce the power consumption of the generated signals with stable frequency of oscillation. The expected PUF activation time will be much smaller than the total chip lifetime. The proposed PUF utilizes the positive temperature coefficient of the current starved inverters to offset the response instability due to the negative temperature coefficient of the regular

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

inverters used in the classic RO PUF. The new RO-PUF can be used to increasing maximum number of possible challenge/response pairs; and to generate a high number of bits while consuming lower area; then improve the reliability of PUF in case of temperature variations[2]. The frequency of the RO will be inversely proportional to the operation time in years. Two types are commonly used to increase the oscillation frequency. Firstly, functional voltage may be increased. This increases both the oscillation frequency and the current. The maximum acceptable voltage applied to the circuits which limits a given oscillator speed. Secondly, a smaller number of inverters collapsed to form a ring which results in a higher frequency of oscillation given power limitation. RO-PUF can support a high number of challenge/response pairs without affecting the area of the PUF [3].

II. RING OSCILLATOR PUF

The basic RO PUF consists of two matching ring oscillators, which due to invention variation will have small distinction in delay. One bit can be defined by comparing the speed and this bit will be equally to be a zero or a one as long as the fabrication variation is random. However, the bit we extract from a pair of ROs this way may not be reliable and unclonable. For example, operating environment such as temperature and voltage has significant impact on delay. When this impact is sufficiently large, it becomes possible that the same RO is faster or slower which depends upon the temperature at one stage or at another stage, causing the bit generated from this pair of ROs to flip when temperature changes [4]. The maximum number of challenge/response pairs is raised to

$$CRP = \frac{R(R-1)}{2} * L^{C} \qquad (1)$$

Where R is denoted as number of ring oscillators, C represents number of columns and L indicates number of supply voltages. The number of stages in a ring oscillator is the number of inverters in the feedback loop. The ring oscillator generates a clock signal, the frequency of which is directly related to the delay of the inverters. The outputs of the ring oscillators are connected to the inputs of two N−to−1 multiplexers. A (2 log2) N-bit challenge selects a pair of ring oscillators, the outputs of which will be connected to the clock inputs of the two counters. The two counters will start counting at the same time and after a specific period of time (determined by the Ref Counter as a Run Time), the counter outputs are compared. If the upper counter has a greater value, the response bit will be 0, otherwise 1. Theoretically, the oscillation frequency of all the ring oscillators should be the same because they are identical. However, due to the inherent interchip and intra-chip process variations, as well as the environmental conditions, the delays of the inverters will vary across different ring oscillators, thus affecting the oscillation frequency of the ROs. For bit generation the form of fastest and slowest ROs in each unit are picked. This type uses two ROs with large speed difference.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

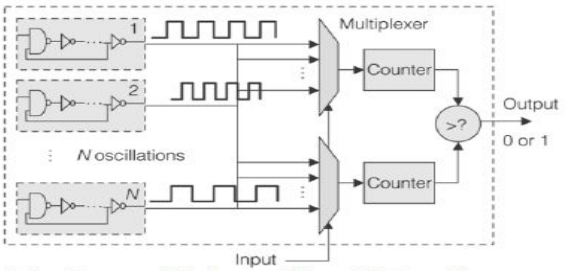

Fig 1 1-out-of-N ring oscillator PUF architecture

Compare frequencies of two oscillator is randomly determined by manufacturing variations. They use Number of ROs multiplexers, counters, and comparators these make this approach very hardware expensive. Another known weakness of RO PUF is that it is subject to the negative effect of correlated or systematic variation, which weakens the security of PUF secret. The disadvantages of this design is the low ratio of the number of response bits to the number of challenge bits (1/2 log 2N). Physical Unclonable Functions (PUFs) is a device of an FPGA [5]. This design can be somewhat simple given the structure of the ROs of several NOT gates connected serially. In this implementation, I used the challenge bits to select two of 16 ROs available in the circuit. To select the oscillators, I split the challenge in two 4- bit parts, each used as the controller signals for two 16:1 MUXes. Both MUXes are connected to the same ROs but in different order. As soon as one of the counters overflows, the counting is stopped and one bit of the output of the PUF is calculated. For this calculation some use a comparator. The maximum number of possible comparisons between N different ROs is equal to: N× (N−1)/2 Oscillation Frequency of RO is

$$F_{osc} = \frac{1}{2 * N * Delay} \qquad (2)$$

the oscillation frequency of different ring oscillators to compute the output bits [6]. The new design of RO PUF consumes lower power and area than conventional methods.

III. PROPOSED SYSTEM

The 8-bit linear feedback shift register is applied to antifuse algorithm. A linear feedback shift register is also called a shift register that can be formed by performing XOR on the outputs of two or more flip-flops together and feed those outputs back into the input of one flip-flops. The repeating progression of states of a LFSR allows it to be used as a clock divider [7]. For test-pattern generation LFSRs are used in circuit testing. LFSR performs whose input bit is a linear function of its prior state. The most usually used linear function of single bits is XOR. A LFSR is most regularly a shift register whose input bit is driven by the XOR of some bits of the general shift register value. The consequences illustrate that the frequency of hybrid RO is least susceptible to temperature variations [8]. Both Synchronous and Asynchronous counters are able to counting "Up" and "Down" by Bidirectional Counter. It is a "Universal" type of counter that using an additional control input to count in both directions depending on the state of their input control pin. A simple N-bit Up/down synchronous counter using JK flip-flops designed to operate as toggle or act as a T-type flip-flops for giving a maximum count of (000) to (111) in binary mode and carry to zero again. Most of the bidirectional counter chips can be made to change their

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

count route either up or down at any point within their counting progression which is achieved by using an additional input pin and it determines the direction of the count, either up or down. Bidirectional counter which accepts forward pulse and reverse pulse counts in any chain without any dedicated circuits. A number of consecutively connected binary flip-flops with the output of the first provides the input for the second, the output of the second providing the input for the third. To obtain a decimal output warning, four flip-flops are connected in series combination together with complex feedback connections between selected stages so that ten pulses applied to the input of the cascaded flip-flops is efficient, to generate an output indication upon the relevance of the tenth pulse rather than upon the application of the sixteenth pulse as would result if feedback were not employed.

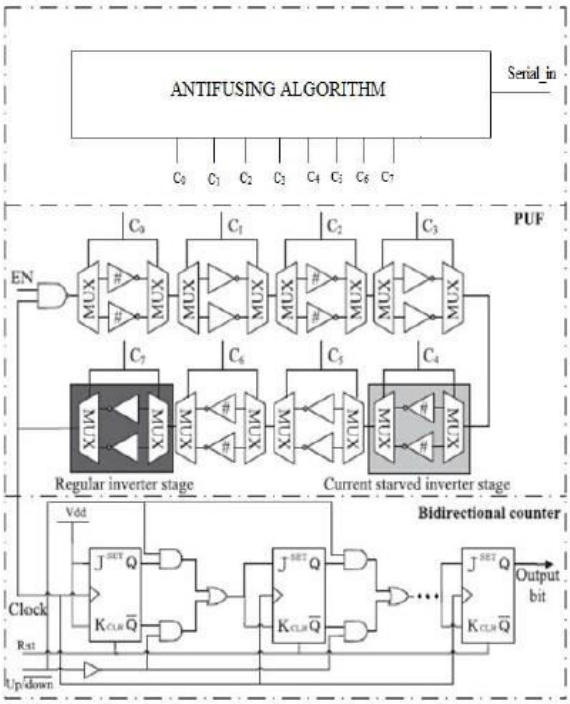

Fig 2 Proposed RO PUF system

A Bidirectional Counter comprise,

(a) A plurality of flip-flops having first and second inputs and first and second outputs;

(b) First means plausibly connecting the first output of all but one of said flip-flops to the second input of its resultant flip-flop and the second output of all but said one flip-flop to the first input of said resultant flip-flop.A PUF circuit contains NAND gate which is equivalent to a regular inverter when EN is asserted. Each stage inverters are covered with two multiplexers. The multiplexors are used to reduce their delay and transistor count. Fig 2 shows the CMOS circuit implementation of a hybrid RO PUF with Antifuse algorithm.

Antifuse Algorithm:

```
initial address= (N/2);
for (i=log(N/2),i>0,i--)
{
        if(|address|= =1)
                address= address+1;
        if(|address|= =0)
                address= address-1, $stop;
        else
                address= address-1;
                address= address+2^(i-1);
        else
                address= address-2^(i-1);
}
```

A shadow challenge CB is generated from the LFSR counter after, (< 28) clock cycles. With a well-chosen feedback function, the LFSR counter will produce a pseudo random sequence with a very long cycle and CB≠CA. After CB is stable, High value is lay down to EN. With the same counting time t, the value stored in the counter is really proportional to the frequency variation of the two selected ROs, i.e., Δf = fA−fB the most significant bit of the counter is the output bit of the PUF [9]. The length of the bidirectional counter has to be large enough to differentiate the two uninterrupted

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ROs frequencies the same input challenge can generate a different response with a different. This structure can be related to a logically reconfigurable PUF [10] for increasing the security of the PUF. It allows the challenge/response pair (CRP) activities to be changed by changing without physically replacing PUF. If logicalreconfigurability is not required, CA and CB can be fed successively without the LFSR. Our method can be used for: Designing low-power hybrid RO PUF with latency limitations using Antifuse algorithm. Improving the RO-PUF reliability by decreasing its sensitivity to temperature variations [11] [12]. The proposed system is to improve the system performance level by reducing the delay and less consumes of power. Our method can be used for: Designing low-power hybrid RO PUF with latency limitations using antifuse algorithm. Improving the RO-PUF reliability by decreasing its sensitivity to temperature variations. The proposed system is to improve the system performance level.

IV. RESULTS AND DISCUSSION

The proposed system architecture is designed using verilog HDL, Use modelsim software for simulated and Xilinx project navigator for synthesized process. The RTL schematic view is illustrated in fig 3 and its Technology schematic view is displayed in fig 4.

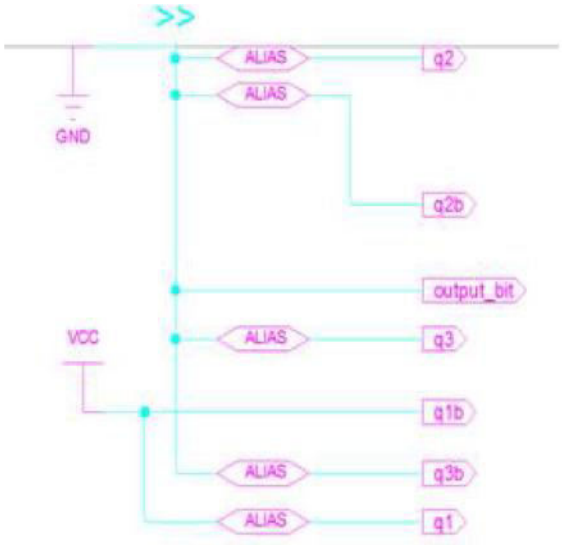

Fig 3 RTL Schematic view

The above figure shows the designed perspective view of the proposed project. It consists of input ports and output ports.

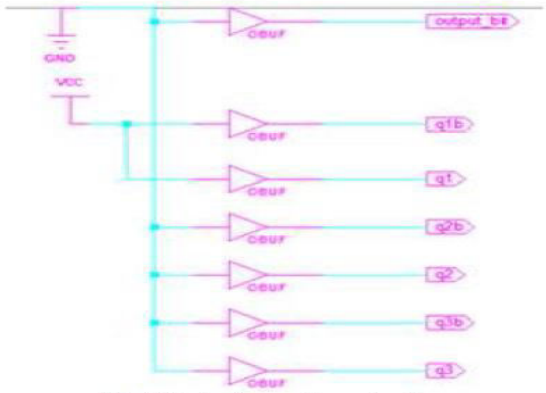

Fig 4 Technology schematic view

The input pin is represented as 'serial input' and output pin is renowned as 'output bit'. After the optimization and technology target phase of the separation process, use the Technology Viewer to view a schematic design of a circuit in terms of logic elements optimized to the Xilinx device, for example, in terms of Look-Up-Tables, carry logic, I/O buffers, and some specific components.

(a) Delay Measurement:

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

The Fig 5 shows that all inputs, outputs and internal variables used in this project and its all indicates with low (0) and high (1) values. The address of Antifusing was declared. And also it shows the delay values in ps.

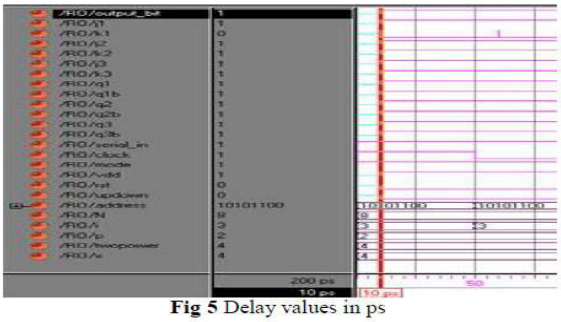

Fig 5 Delay values in ps

(b) Power Measurement:

```
Power summary:                          I(mA)     P(mW)
---------------------------------------------------------------
Total estimated power consumption:                   52
                                        ---
                          Vccint 1.20V:     15       19
                          Vccaux 2.50V:     12       30
                          Vcco25 2.50V:      2        4
                                        ---
                              Outputs:
                                Vcco25      0        0
                              Signals:      0        0
                                        ---
                    Quiescent Vccint  1.20V:     15       19
                    Quiescent Vccaux  2.50V:     12       30
                    Quiescent Vcco25  2.50V:      2        4

Thermal summary:
---------------------------------------------------------------
   Estimated junction temperature:                   27C
                       Ambient temp:  25C
                          Case temp:  26C
                         Theta J-A:  37C/W
```

Fig 6 Power analysis report

The above diagram shows total estimated power consumption of 52mW. There are slightly change in temperature also. These terms are found out using power analysis tool.

Performance comparisons

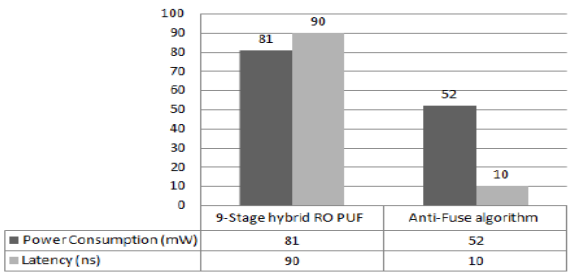

Fig 7 Graphical comparisons with conventional results

The fig 7 shows graphical representations of the 9-Stage hybrid RO PUF and Antifusing results of power consumption and delay measurements. The exact values are plotted on the graph. Then the existing method consumes 81mW of power and proposed method consumes 52 mW of power for the designed project. The delay values will be reduced up to 90%.

V. CONCLUSION

A low-cost RO PUF with improved thermal stability has been presented. The proposed PUF utilizes the positive temperature coefficient of the current starved inverters to offset the response unsteadiness due to the depressing temperature coefficient of the regular inverters used in the classic hybrid RO PUF. In this proposed work, Antifuse Algorithm is used to reduce the power consumption of the generated signals with stable frequency of oscillation. This project concentrates on the delay and power consumption respectively 10ps and 52mW. The results show that the frequency of hybrid RO is less adaptable to the temperature certain a range is 27◦C.

REFERENCES

[1]Yuan Cao," A Low-Power Hybrid RO PUF With Improved Thermal Stability for Lightweight Applications", IEEE Transactions On Computeraided Design Of Integrated Circuits And Systems, Vol. 34, No. 7, July 2015.

[2]L.Zhang, Z.H.Kong, "Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions," IEEE Trans.

Inf. Forensics Security, vol. 9, pp. 921–932, Jun. 2014.

[3]S. Mansouri and E. Dubrova, "Ring oscillator physical unclonable function with multi level supply voltages," in Proc. IEEE 30th Int. Conf. Comput. Design, Montreal, QC, Canada, Sep. 2012, pp. 520–521.

[4]D. Merli, F. Stumpf, and C. Eckert, "Improving the quality of ring oscillator PUFs on FPGA," in Proc. Workshop Embedded Syst. Security (WESS), Scottsdale, AZ, USA, Oct. 2010, pp. 1–9

[5]Chi-En Yin and Gang Qu "Design and Implementation of a Group-based RO PUF" EDAA 2012.

[6]E. Socher, S. Beer, and Y. Nemirovsky, "Temperature sensitivity of SOI-CMOS transistors for use in uncooled thermal sensing," IEEE Trans. Electron Devices, vol. 52, no. 12, pp. 2784–2790, Dec. 2005.

[7]Y. Su, J. Holleman, and B. Otis, "A 1.6 pj/bit 96% stable chip-ID generating circuit using process variations," in Proc. IEEE Int. Solid-State Circuits Conf., San Francisco, CA, USA, Feb. 2007, pp. 406–407.

[8]R. Kumar, H. Chandrikakutty, and S. Kundu, "On improving reliability of delay based physically unclonable functions under temperature variations," in Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on, June 2011, pp. 142 –147.

[9]A. Maiti, P. Schaumont, "Improving the quality of a Physical Unclonable Function using configurable Ring Oscillators," FPLA 2009.

[10]G. E. Suh, S Devadas, "Physical Unclonable Functions for Device" in RFID, pp. 15-19, May 2010.

[11]R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way functions," Science, Sep 2002.

[12]S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based "unclonable" RFIDS for anticounterfeiting and security applications," in RFID, pp. 58-64, April 2008.