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 2nd Sept 2017. Link :http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-7

Title: **HIGH EFFICIENT LOW-POWER HYBRID RO PUF FOR LIGHTWEIGHT APPLICATIONS STABILITY WITH ENHANCED THERMAL**

Volume 06, Issue 07, Pages: 663 – 669.

Paper Authors

V.TEJASRI, B.NAGAIAH

Krishnaveni Engineering College for Women, Kesanupalli,AP,India

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

HIGH EFFICIENT LOW-POWER HYBRID RO PUF FOR LIGHTWEIGHT APPLICATIONS STABILITY WITH ENHANCED THERMAL

[1]V.TEJASRI, [2]B.NAGAIAH

[1]M.Tech Student, Krishnaveni Engineering College for Women, Kesanupalli,AP,India

[2]Assistant Professor, Krishnaveni Engineering College for Women, Kesanupalli,AP,India
[1]tejasri.vutukri.@gmail.com,[2]b.nagaiah2@gmail.com

Abstract: Ring oscillator (RO)- based physical unclonable capacity (PUF) is versatile against commotion impacts, however its reaction is powerless to temperature varieties. This paper exhibits a low-power and little impression half breed RO PUF with a high temperature soundness, which makes it a perfect possibility for lightweight applications. The negative temperature coefficient of the low-control sub edge operation of current starved inverters is misused to alleviate the varieties of differential RO frequencies with temperature. The new design utilizes obviously streamlined hardware to create and think about countless of RO frequencies. The proposed nine phase half breed RO PUF was created utilizing worldwide foundry 65-nm CMOS innovation.

Keywords Physical Un Clonable Function, Ring Oscillator, Bi-Directional Counter, Temperature Stability.

I. INTRODUCTION

Physical Unclonable Functions (PUF) is an inventive circuit primitive that concentrate mystery key from physical attributes of incorporated circuits. At first, Ring oscillator based physical unclonable capacity is versatile against commotion impediments yet its reaction is much versatile to temperature varieties [1]. RO-PUF is better than other siliconbased PUFs. The unconstructive temperature coefficient of the low-control sub limit operation of current starved inverters is abused to part the varieties of differential RO frequencies with temperature changes. Afterward, another structure to create secure PUF confirms from ring oscillator (RO) PUF with enhanced equipment proficiency. Controller is utilized to create the control flag which controls the focused on RO and reference RO. Antifusing Algorithm is utilized to decrease the power utilization of the produced signals with stable recurrence of swaying. The normal PUF actuation time will be substantially littler than the aggregate chip lifetime. The proposed PUF uses the positive temperature coefficient of the current starved inverters to counterbalance the reaction flimsiness because of the negative temperature coefficient of the consistent inverters utilized as a part of the exemplary RO PUF. The new RO-PUF can be used to increasing maximum number of possible challenge/response pairs; and to generate a

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

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 essential RO PUF comprises of two coordinating ring oscillators, which because of innovation variety will have little qualification in delay. One piece can be characterized by looking at the speed and this bit will be similarly to be a zero or a one as long as the manufacture variety is arbitrary. Be that as it may, the bit we separate from a couple of ROs along these lines may not be dependable. what's more, unclonable. For instance, working condition, for example, temperature and voltage has huge effect on delay. At the point when this effect is adequately huge, it ends up plainly conceivable that a similar RO is quicker or slower which relies on the temperature at one phase or at another stage, causing the bit created from this combine of ROs to flip when temperature changes [4].The maximum number of challenge/response pairs is raised to CRP = R(R − 1) 2 ∗ L (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 (2log2) 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.

III. EXISTING METHOD

The classic RO PUF is made of two N-to-1 multiplexors, two counters, one comparator, and N identical ROs, as shown in Fig. 1(a).

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

Due to the inter and intrachip process variations, the frequency of each RO differs. A 2 log2 N-bit challenge is input to the two multiplexors to select a pair of ROs. Depending on which of the selected ROs has a larger frequency, the response bit of the PUF is either 0 or 1. Therefore, the greater the difference between the oscillation frequencies of any RO pair, the more reliable is the output response bit of the PUF. A 1-out-of-k masking scheme is adopted in [5], where groups of k five-stage ROs with k = 8 are implemented. A stable response bit is derived by selecting the pair of ROs in a group that has the maximum frequency difference. The reliability is improved over the classic RO PUF by requiring k × n ROs for an n-bit response. In [9], each RO is replaced by a configurable RO in a CLB of a field programmable gate array (FPGA). The configurable design enables k instead of one RO pair to be formed between two CLBs. Similar to the 1-out-of-k masking scheme, the pair that has the maximum distance among k RO pairs is selected. High reliability is achieved at the cost of substantial hardware redundancy.

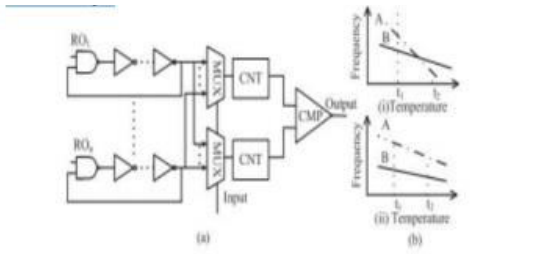

Fig.1. (a) Classic RO PUF architecture. (b) Output bits of two different temperature induced frequency distance scenarios of two RO pairs: the output bit (i) flips and (ii) is stable.

The dynamic variation of the oscillation frequency with temperature is a major concern for the response bit stability. The output frequency of the oscillator is inversely The dynamic variation of the oscillation frequency with temperature is a major concern for the response bit stability. The output frequency of the oscillator is inversely

$$t_d = \frac{C_0 V_{dd}}{\eta I_D} \qquad (1)$$

where C0 is the total load capacitance, Vdd is the power supply voltage, ηID is the mean current (disregard leakage and short circuit current), η is a fixed parameter for a given inverter and ID is the saturation current. To a crude approximation, ID is given by [11]

$$I_D = \frac{\mu C_{OX} W}{2L}(V_{GS} - V_t)^2 \qquad (2)$$

where W, L, VGS, COX, Vt, and μ are the effective channel width and length, gate-to-source voltage, gate capacitance, threshold voltage and charge carrier mobility, respectively.

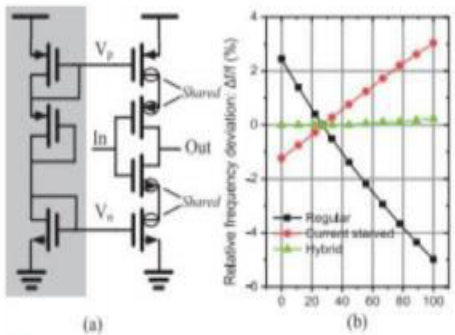

Fig.2. (a) Current starved inverter circuit. The diffusion regions can be shared with other transistors, and the bias voltages Vp and Vn can be provided externally or generated internally by a common circuit in the shaded block. (b) Relative frequency deviations against temperature for three ROs with nine stages of regular, current starved, and hybrid inverters, respectively.

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

From (2), the temperature coefficient of switching current TCC [12] can be derived as

$$TCC = \frac{1}{I_D}\frac{dI_D}{dT} = \frac{1}{\mu}\frac{d\mu}{dT} - \frac{2}{V_{GS}-V_t}\frac{dV_t}{dT} \quad (3)$$

The temperature dependent parameters, Vt and μ, are expressed as [2]

$$V_t(T) = V_t(T_0) - \sigma(T - T_0) \quad (4)$$

$$\mu(T) = \mu(T_0)\left(\frac{T}{T_0}\right)^{\kappa} \quad (5)$$

where T0 is the reference temperature. κ and σ are, respectively, the mobility temperature exponent in the range of 1.2–2 and the threshold voltage temperature coefficient in the range of 0.5–3 mV/K. The threshold voltage Vt(T) decreases with increasing temperature, resulting in a rising drain saturation current as temperature increases. On the contrary, the mobility of charge carriers decreases with increasing temperature, which in turn reduces the drain saturation current. The reduction in carrier mobility is more prominent than the reduction in threshold voltage in the super-threshold operation region. Consequently, the delay of a regular inverter gate exhibits an overall positive temperature dependence relation.

IV. PROPOSED TEMPERATURE COEFFICIENT COMPENSATED HYBRID-INVERTER-BASED RO PUF

By adding two transistors to the regular inverter circuit, the MOSFET transistors of the current starved inverter circuit in Fig. 2(a) can be made to operate in the subthreshold region by adjusting the bias voltages Vp and Vn. The drain current can be expressed as

$$I_{D,sub} = \mu C_{OX}\frac{W}{L}\left(\frac{\kappa_B T}{q}\right)^2 (n-1)e^{\frac{q(V_{GS}-V_t)}{n\kappa_B T}}\left(1 - e^{-\frac{qV_D}{\kappa_B T}}\right)$$

$$n = \frac{1 + (C_S + C_{it})}{C_{OX}}$$

where κB is a temperature independent coefficient. CS, Cit, and Cox are the capacitance associated with the semiconductor, fast surface states, and gate oxide, respectively. The temperature coefficient of the switching current TCCsub can be formulated as [12]

$$TCC_{sub} = \frac{1}{u}\frac{d\mu}{dT} + \frac{2}{T} - \frac{q}{n\kappa_B T}\left(\frac{dV_t}{dT} + \frac{V_{GS}-V_t}{T}\right) \quad (7)$$

TABLE I: Comparison of Regular, Current Starved, And Hybrid RO

Type of RO	Regular	Current starved	Hybrid
Power (μW)	58.07	20.75	23.93
Transistor number	20	36	28
Temperature sensitivity (kHz/°C)	−3160	620	40

Since the decrease of threshold voltage dominates the decrease of mobility with increasing temperature in the sub threshold region, the value of TCCsub is negative [12]. As a result, the delay of a current starved inverter stage decreases with increasing temperature. Based on the above analysis, the positive temperature coefficient effect of the current starved inverters can counteract the negative temperature coefficient effect of the regular inverters of the classic RO PUF. Fig. 2(b) shows the

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

simulation results of the relative frequency deviations (with reference to the frequency at 27 ◦C) versus temperature for the regular, current starved and hybrid ninestage ROs in global foundry (GF) 65-nm CMOS technology. The hybrid RO is made up of five regular inverters and four current starved inverters. The results show that the frequency of hybrid RO is least susceptible to temperature variations. The characteristics of these three types of nine-stage ROs are summarized in Table I. The temperature sensitivity is defined as the output frequency deviation per degree Celsius. The results show that the hybrid RO has a much lower power consumption and temperature sensitivity than the regular RO but uses eight more transistors. These additional biasing transistors can be sized smaller and share their diffusion areas with other transistors to reduce the area overheads The architecture of the proposed (n + 1)-stage (n is even) hybrid RO PUF consists of an n-bit linear feedback shift register (LFSR) counter, a bidirectional counter, a two-input NAND gate, (n/2) regular inverter stages, and (n/2) current starved inverter stages. Fig. 3 shows the CMOS circuit implementation of a nine-stage hybrid RO PUF. The NAND gate is equivalent to a regular inverter when EN is asserted. Two multiplexors are placed before and after the inverters in each stage. The multiplexors are realized with transmission gates to reduce their delay and transistor count. The two multiplexors in each stage share the same select signal, which is one of the 8 bits of the challenge C. This select signal picks up either the upper or lower inverter output, and 28 different possible combinations of inverter path for the RO can be selected. Each response bit of this PUF is generated by the comparison of two selected ROs' frequencies. Fig. 4 shows the timing diagram of its operation. First, the LFSR counter is initialized by shifting an 8-bit challenge CA through the Serial_In port with the Mode signal asserted. The enable line EN of the PUF is set to low to disable the RO. After a small delay when CA is loaded into the LFSR, EN is pulled high and the bidirectional counter is reset by Rst.

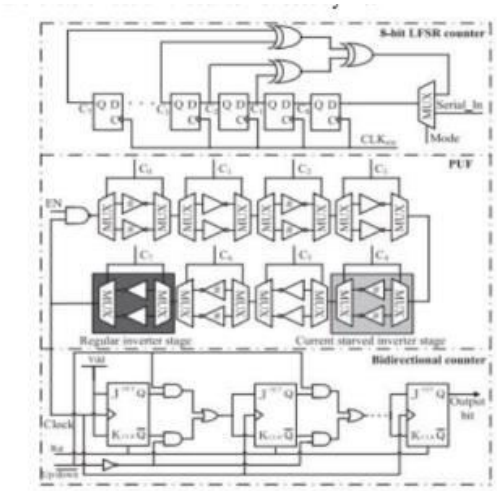

Fig. 3. Architecture of the proposed hybrid RO PUF.

The selected ROA starts to ring and its output is connected to the clock input of the bidirectional counter. The bidirectional counter is con- figured as an up counter by setting the Up/down signal high. The counter value is registered after a specific time t determined by the frequency fA of ROA. Then, EN is set to low. The bidirectional counter is then configured as a down counter by setting Up/down signal low. Next, a shadow challenge CB is generated from the LFSR counter after Nclk

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

(Nclk < 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, EN is set to high. With the same counting time t, the value stored in the counter is directly proportional to the frequency difference of the two selected ROs, i.e., f = fA−fB. The most significant bit of the counter is the output bit of the PUF. The length of the bidirectional counter has to be large enough to discriminate the two successive ROs frequencies. The same input challenge can generate a different response with a different Nclk. This structure can be regarded as a logically reconfigurable PUF [13] for increasing the security of the PUF. It allows the challenge response pair (CRP) behavior to be changed by changing Nclk without physically replacing or modifying the underlying PUF. If logical reconfigurability is not required, CA and CB can be fed successively without the LFSR.

A. Reliability of the Proposed Hybrid RO PUF The reliability measures how reproducible or stable are the CRPs of a PUF under varying operating conditions. It can be measured by its bit error rate (BER) by comparing the responses taken at different time with a reference response to the same challenge. Let Ri be an n-bit response to an input challenge C produced by the PUF of a chip i under a nominal operating condition. The same set of challenges are then applied k times to the same PUF under varying environmental conditions to obtain the responses Ri,j for j = 1, 2,..., k. The reliability S of chip i can be computed by

$$S = 1 - \mathrm{BER} = 1 - \frac{1}{k}\sum_{j=1}^{k}\frac{\mathrm{HD}(R_i, R_{i,j})}{n} \times 100\% \quad (9)$$

The reliability is measured using 1000 CRPs generated bythe PUF under varying supply voltages and temperatures. Fig.6(a) shows the reliability of the fabricated hybrid RO PUF against the voltage variations. Voltage regulatorand voltagelimiter are typically used in modern application-specifiedintegrated circuit design to minimize the supply voltagevariations. With regulated voltage changes of ±2% from 1.2Vnominal supply, the worst reliability is 98.26%. Fig. 6(b)shows the average reliability of the five hybrid RO PUF chipsmeasured by the thermal station. The working temperature isvaried from −40 ◦C to 120 ◦C, with 27 ◦C as the referencetemperature. The average reliability measured from the hybridRO PUF chips is as high as 99.84% and the worst-casereliability is 98.28% at −40 ◦C. The results attest that thefrequency of hybrid RO is much less susceptible totemperature fluctuation. Comparing with the worst-caseeliability of 82% at 100 ◦C reported in [2] for the classic ROPUF, our proposed RO PUF has increased its temperaturereliability by more than 16%.

V. CONCLUSION

A low-cost RO PUF with improved response stability hasbeen presented. The proposed PUF utilizes the positivetemperature

coefficient of the current starved inverters tooffset the response instability due to the negative temperaturecoefficient of the regular inverters used in the classic ROPUF. The prototype PUF chip fabricated in GF 65-nm CMOStechnology consumes only 32.3 µW per CRP at 1.2 V with aworking frequency of 230 MHz. The measured CRPs show anearly perfect average interdie HD of 50.46% and an averageBER of 0.16% with temperature varied from −40 ◦C to 120◦C. The proposed PUF stands out as an ideal candidate forlightweight security applications by comparing its overallfigures of merit with other existing PUFs.

VI. REFERENCES

[1] S. Devadas et al., "Design and implementation of PUFbased'unclonable' RFID ICs for anti-counterfeiting andsecurity applications," in Proc. IEEE Int. Conf. RFID, LasVegas, NV, USA, Apr. 2008, pp. 58–64.

[2] R. Kumar, V. Patil, and S. Kundu, "On design oftemperature invariant physically unclonable functions basedon ring oscillators," in Proc. IEEE Comput. Soc. Annu. Symp.VLSI (ISVLSI), Amherst, MA, USA, Aug. 2012, pp. 165–170.

[3] K. Lofstrom, W. Daasch, and D. Taylor, "ICidentification circuit using device mismatch," in Proc. IEEEInt. Solid-State Circuits Conf. (ISSCC), San Francisco, CA,USA, Feb. 2000, pp. 372–373.

[4] J. W. Lee et al., "A technique to build a secret key inintegrated circuits for identification and authenticationapplication," in Proc. Symp. VLSI Circuits, Honolulu, HI,USA, Jun. 2004, pp. 176–179.

[5] G. Suh and S. Devadas, "Physical unclonable function fordevice authentication and secret key generation," in Proc.44th IEEE Design Autom. Conf. (DAC), San Diego, CA,USA, Jun. 2007, pp. 9–14.

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

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

[8] C. Yin and G. Qu, "Temperature-aware cooperative ringoscillator PUF," in Proc. IEEE Int. Workshop Hardw.-Orient.Security Trust, San Francisco, CA, USA, Jul. 2009, pp. 36–42.

[9] A. Maiti and P. Schaumont, "Improving the quality of aphysical unclonable function using configurable ringoscillators," in Proc. Int. Conf. Field Program. Logic Appl.,Prague, Czech Republic, Aug. 2009, pp. 703–707.

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