Duty-Cycle-Based Controlled Physical Unclonable Function

Mahmood J. Azhar, *Member, IEEE*, Fathi Amsaad, *Member, IEEE*, and Selçuk Köse, *Member, IEEE*

***Abstract*— Physical unclonable functions (PUFs) provide a unique signature based on the variations during the fabrication process of the integrated circuits. The additional features of controllability and reconfigurability to a PUF implementation enable the reuse of the existing hardware as a new modified PUF, enhancing the capabilities of a PUF for more versatile security applications. In this paper, a variable duty-cycle-based ring oscillator circuit is proposed as a controlled and reconfigurable PUF primitive. One of the distinguishing features of the proposed PUF is that duty cycle comparisons are used, instead of the conventional frequency comparisons to generate the output bit response. The advantages of the utilizing duty cycle over the conventional frequency-based comparisons are investigated. The feasibility of the proposed PUF is evaluated using existing figures of merit providing a uniqueness of 49.3%, temperature reliability greater than 92% between 0 and 100 °C, and supply voltage reliability greater than 96% between 0.9 and 1 V.**

***Index Terms*— Configurable, controllable, duty cycle, hardware security, physical unclonable function (PUF), reliability, ring oscillator.**

I. Introduction

PHYSICAL unclonable functions (PUFs) are widely used as hardware security primitives to provide a unique signature for device authentication and secret key generation. PUFs have been utilized as an alternative to improve the security of the secret hardware keys stored in nonvolatile memory blocks in integrated circuits (ICs) that are potentially vulnerable to external attacks [1]–[3]. Additionally, PUFs offer dynamic circuit architectures that generate a device signature based on the random nature of circuit delay variations determined by the random manufacturing process variations as an alternative to fixed identification signatures stored within ICs [3], [4]. A list of process parameter variations that may impact the delay and leakage characteristics of CMOS-based digital circuits, and accordingly utilized in PUFs, is provided in [5] and [6].

The two primary delay-based PUF topologies are the arbiter PUF and ring oscillator PUF (ROPUF) [4], [7]–[9]. An arbiter PUF provides a rich set of challenge and response pairs as compared to an ROPUF, but suffers from higher vulnerability to attacks such as the model development through machine learning techniques [7], [9]. Alternatively, a conventional ROPUF, as shown in Fig. 1, utilizes a group of electrically and geometrically identical ring oscillators that are randomly distributed throughout an IC. The frequency of the oscillation is used for comparison to generate the output response bits which may suffer from reliability issues due to temperature and voltage variations [3], [4]. Several techniques and algorithms have previously been proposed to ensure a distinct selection of frequency pairs with a separation that is greater than the noise threshold [10], [11]. A conventional PUF that allows direct user access is potentially vulnerable to man in the middle attacks [12]. A controlled PUF has been proposed in [12], where the PUF is used to generate random responses through a dedicated secure programming interface. The PUF challenges and responses are controlled through a secure CPU interface using one-way hash functions, isolating the PUF from a possible direct external attack by an adversary [12]. An important requirement of a controlled PUF is the ability to accept digital inputs and produce random output bits. Typical applications of controlled PUF are explored in [12] and [13].

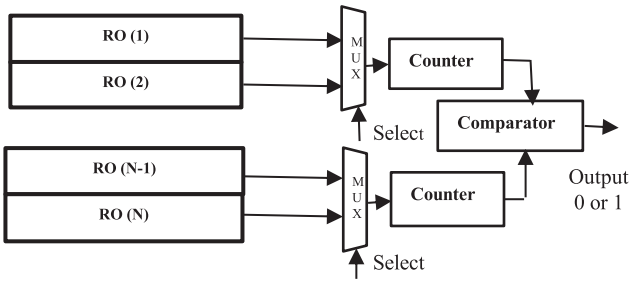

Fig. 1. Architecture of a conventional ROPUF.

A variety of reconfigurable PUFs have been proposed in [8] and [16] to reuse the PUF architecture for enhancing security either by increasing the number of challenge response pairs or enhancing the security against certain attacks with a new PUF configuration. In addition, reconfigurable PUFs may also offer power consumption and speed tradeoff [17].

The proposed duty-cycle-based controlled PUF primitive can be used as a controlled and reconfigurable PUF. The controllability and reconfigurability properties of the proposed

Manuscript received September 27, 2017; revised February 13, 2018; accepted March 25, 2018. This work was supported in part by the National Science Foundation CAREER Award under Grant CCF-1350451, in part by the National Science Foundation Award under Grant CNS-1715286, and in part by the Cisco Systems Research Award. *(Corresponding author: Mahmood J. Azhar.)*

M. J. Azhar and S. Köse are with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: mazhar@mail.usf.edu; kose@usf.edu).

F. Amsaad is with the Department of Computer Science and Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: famsaad@usf.edu).

Digital Object Identifier 10.1109/TVLSI.2018.2827238

PUF are extensively studied both theoretically and with circuit analysis and simulations. The proposed PUF primitive provides the features of reconfigurable operation [16] that enables the generation of additional challenge response pairs, thus optimizing the area and enhancing security. The analysis of the proposed PUF primitive to demonstrate resistance to man-in-the middle, side channel, and fault injection attacks is, however, not in the scope of this paper.

A. Contributions of This Paper

The proposed controlled PUF primitive utilizes a ring oscillator with current-starved pull-up stages [14], [18]. This controlled ring oscillator generates a wide range of frequencies and duty cycles with the digital control and is shown to be stable under process, voltage, and temperature (PVT) variations. The contributions to this paper are based upon extensive circuit design enhancements to the prior work [14], [18]. The novel contributions of this paper are summarized as follows and are demonstrated with a detailed mathematical analysis and extensive simulations.

1) A duty cycle comparison-based PUF primitive is proposed and demonstrated to be reliable over voltage and temperature (VT) variations.
2) The proposed PUF primitive provides enhanced random duty cycle spread based on process variability and circuit features on the chip, and has a potential to provide an increased number of challenge/response pairs with negligible area and power overhead.
3) The proposed PUF primitive may be digitally reconfigured to provide a new set of random duty cycle values.

B. Background Work and Comparisons

Using the delay mismatch in ring oscillators as a basis to develop a duty-cycle-based PUF has previously been proposed in [15]. This technique relies on the mismatch of the transistor width-to-length ratio between inverter stages and uses 15 inverter stages in the ring oscillator for PUF implementation. Using a long chain of inverters in a ring oscillator produces a lower random statistical duty cycle spread and leads to higher power consumption and area due to the large MOS transistor widths as described in Section II-A. The PUF proposed in [15] uses the duty cycle at the intermediate nodes of a mismatched inverter chain. The duty cycle values have a nonuniform intersecting temperature profile which can result in low entropy and reduced reliability due to flip-bit errors [3], [4].

Alternatively, the proposed duty-cycle-based PUF can be digitally configured to operate over a wide range of duty cycle values from 20% to 90% with a high granularity and is demonstrated to provide a VT stable output. Uniform sized seven inverter stages are incorporated in a circuit topology to amplify the statistical spread of random distribution of the duty cycle using a feedback circuit. The increased statistical variations of the duty cycle provide a wider range of distinct duty cycle values. The digital inputs are used to mitigate for the temperature and voltage variations. The current starved inverters enable a low power operation.

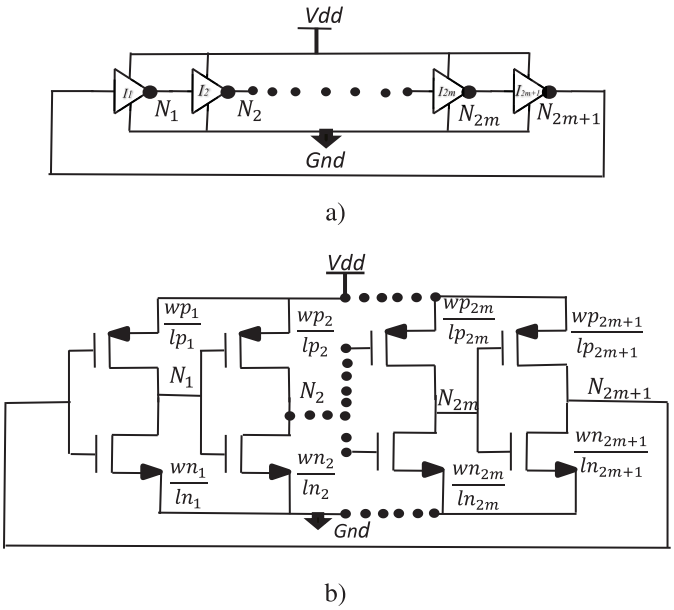

Fig. 2. Typical ring oscillator circuit. (a) Ring oscillator circuit with $(2m+1)$ inverter stages. (b) Transistor level schematic of a $(2m+1)$ stage ring oscillator.

C. Paper Organization

A detailed comparison between different PUF topologies that utilize either duty cycle or frequency is offered in Section II. The prior work on PVT-stable pulsewidth modulator (PWM) that is used as a foundation for implementing the proposed duty cycle PUF is described in Section III. The proposed duty-cycle-based ring oscillator and the techniques to enhance the statistical duty cycle spread over process variations are explained with analytical and simulation results in Section IV. In Section V, figures of quality are evaluated and presented with simulation results for the proposed PUF scheme. In Section VI, a comparison of the proposed PUF with the state-of-the-art PUFs is provided. Finally, conclusions are offered in Section VII.

II. Frequency Versus Duty-Cycle-Based PUF

A Monte Carlo analysis of the frequency and duty cycle of a ring oscillator is performed based on a set of Gaussian distributed inverter rise and fall times. The standard deviations of the inverter rise and fall times are obtained through Monte Carlo simulations using 22-nm low power (LP) CMOS predictive technology models (PTMs) [19]. The models are extended to $\pm 3\sigma$ (six sigma) fast-fast (FF) and slow-slow (SS) process corners and the corresponding Gaussian device parameter statistical models [19]. The standard deviations of the inverter rise and fall times obtained through 500 inverter samples are, respectively, 0.055 and 0.042, normalized over a mean value of 1.

A conventional ring oscillator with $2m+1$ inverter stages, where m is an even integer, is shown in Fig. 2(a) and (b). For this ring oscillator, the total active high and low time periods of oscillation, *tph* and *tpl* can be expressed, respectively, as

$$tph = \sum_{i=1}^{(m+1)} tdf(i) + \sum_{i=1}^{m} tdr(i) \tag{1}$$

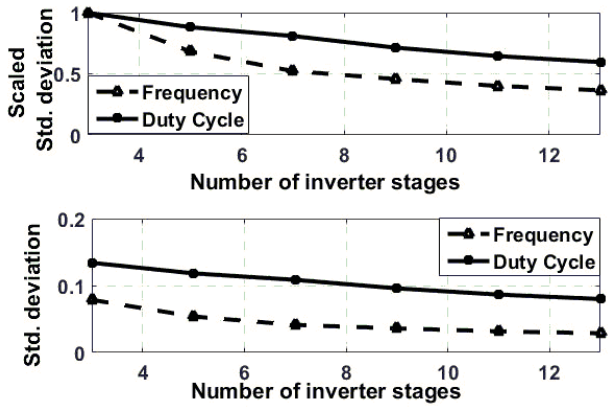

Fig. 3. Standard deviation variations of the frequency and duty cycle for different ring oscillator lengths.

$$tpl = \sum_{i=1}^{(m+1)} tdr(i) + \sum_{i=1}^{m} tdf(i). \tag{2}$$

where $tdf(i)$ and $tdr(i)$ are, respectively, the fall and rise propagation delays of each inverter stage. The results of the Monte Carlo simulations provide an insight into the upper and lower bound estimates of the device process parameters for the variability spread of frequency and duty cycle over the $\pm 3\sigma$ standard deviations.

A. Impact of Number of Inverter Stages

The reduction in the standard deviation of the frequency with larger number of ring oscillator stages has been addressed and discussed in [20]. The impact on the standard deviation of the duty cycle and frequency is examined by varying the number of inverter stages from three to thirteen for the corresponding values of $m = 1$ to 6 using (1) and (2). Monte Carlo analysis of 10 000 samples of ring oscillators are performed using the inverter standard deviation values of 0.055 for the rise time and 0.042 for the fall time to obtain the standard deviation of the frequency and duty cycle. The results are shown in Fig. 3 which are scaled to the value of a three-stage ring oscillator (top) and unscaled values (bottom). The relative decrease in the standard deviation of the frequency is greater than that of the duty cycle when the number of stages increases. The decrease in the standard deviation of duty cycle and frequency is approximately 43% and 75%, respectively. The result suggests that using a smaller number of stages in an ROPUF can lead to higher variability.

The oscillation frequency of a ring oscillator is inversely proportional to the number of stages [4]. Assuming that each inverter stage has the same rise and fall times, the frequency of oscillation of a five-stage and seven-stage oscillator is, respectively, reduced by approximately 60% and 40% as compared to the frequency of a three-stage ring oscillator. Although the three- and five-stage ring oscillators are smaller in area, a higher frequency of operation may require on-chip shielding techniques that would increase the area and power consumption [21]. A seven-stage ring oscillator is, therefore, used in this paper.

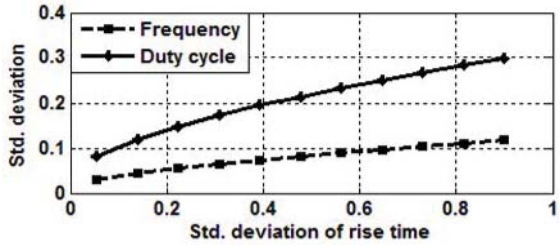

Fig. 4. Standard deviation variations of the duty cycle and frequency of the ring oscillator under varying standard deviations of the inverter rise time.

B. Impact of Inverter Rise and Fall Time Variance on the Variance of Duty Cycle and Frequency

Using (1) and (2), the standard deviation of the frequency and duty cycle is determined as a function of the standard deviation of the rise time of an inverter stage. A Monte Carlo analysis of the duty cycle and frequency is performed using 100 000 Gaussian samples of rise time delay for each inverter stage. The standard deviation of the rise time of an inverter stage is changed from 0.055 to 0.9 over uniform steps with a mean value of 1. The standard deviation of the fall time is 0.042 with a mean value of 1. The results are shown in Fig. 4. The standard deviation of the duty cycle increases more than that of the frequency with an increase in the standard deviation of the rise time of the inverter stages.

C. Improving Duty Cycle Spread Over Process Corners

Increasing the standard deviation of the rise and fall delay mismatch between the inverter stages leads to a higher standard deviation of the duty cycle as compared to a matched ring oscillator, as explained in Section II-B. Assuming a Gaussian distribution for the duty cycle, the increase in the standard deviation of the duty cycle corresponds to an increase in the spread between the upper and lower bounds of $\pm 3\sigma$, SS and FF process corner limits. The increased duty cycle spread over the process corners reduces the probability of intersection of duty cycle values under VT variations, reducing the probability of flip-bit error [3], thus improving reliability.

A seven-stage ring oscillator is used in the analysis. When the rise delay is mismatched by a factor of $k1$ for FF corner and the rise delay is mismatched by a factor of $k2$ for SS corner [see (1) and (2)], the corresponding duty cycle and frequency spreads DS and FS, respectively, can be written in terms of the duty cycle D and frequency F as

$$tpl_{ff} = 4 \times tdr_{ff}(k1) + 3 \times tdf_{ff} \tag{3}$$
$$tph_{ff} = 4 \times tdf_{ff} + 3 \times tdr_{ff}(k1) \tag{4}$$
$$tpl_{ss} = 4 \times tdr_{ss}(k2) + 3 \times tdf_{ss} \tag{5}$$
$$tph_{ss} = 4 \times tdf_{ss} + 3 \times tdr_{ss}(k2) \tag{6}$$
$$DS = D_{ff} - D_{ss} \tag{7}$$
$$FS = F_{ff} - F_{ss}. \tag{8}$$

where the subscripts ff and ss, respectively, refer to FF and SS corners. For $k1 = 1.0$ and $1 < k2 < 2$ in (3)–(6), the variation of the duty cycle and frequency spread between SS and FF corners (i.e., DS and FS) are shown in Fig. 5. The duty

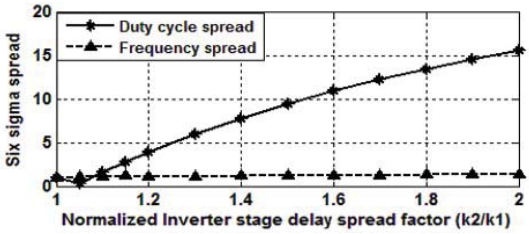

Fig. 5. Frequency and duty cycle spread versus rise time spread.

cycle spread increases considerably over the process corners, whereas the frequency spread reduces as the delay mismatch increases.

D. Mismatched Ring Oscillator Circuit Analysis and Simulation Results

For a typical seven-stage ring oscillator, the time period of the active high, *tph* and low, *tpl* at the output using (1) and (2) can be written as

$$tpl = 4 \times tdr + 3 \times tdf \tag{9}$$

$$tph = 4 \times tdf + 3 \times tdr \tag{10}$$

where *tdf* and *tdr* are, respectively, the fall and rise propagation delays of each inverter stage. The duty cycle is inversely proportional to the ratio of *tpl/tph*. Accordingly, the ratio can be written as

$$\frac{tpl}{tph} = \frac{(4 \times tdr + 3 \times tdf)}{(4 \times tdf + 3 \times tdr)}. \tag{11}$$

For the equal values of *tdr* and *tdf*, the ratio expressed in (11) is one and the duty cycle is 50%. For the case of the fast rise time of odd inverters and slow rise time of even inverters, and the same fall time as that of fast rise time inverters, (11) reduces to

$$\frac{tpl}{tph} = \frac{tdr}{tdf}. \tag{12}$$

The period of the oscillation *tp* can be expressed approximately as

$$tp = (4 \times tdr) + (4 \times tdf). \tag{13}$$

For an inverter implementation using CMOS devices, as shown in Fig. 2, the fall and rise delays can be approximated using MOS α power-law current-based delay expression as

$$tdf = \frac{(vdd * Cl)}{(un * Cox * (Wn/Ln)[(vdd - vtn)^{\alpha}])} \tag{14}$$

$$tdr = \frac{(vdd * Cl)}{(up * Cox * (Wp/Lp)[(vdd - vtp)^{\alpha}])} \tag{15}$$

where *vdd* is the supply voltage, *Cl* is the output load capacitance, Cox is the oxide capacitance, *(Wn/Ln)* and *(Wp/Lp)* are the channel width-to-length ratios for nMOS and pMOS devices, and *vtp*, *vtn*, *up*, *un* are nMOS and pMOS threshold voltages and channel mobility, respectively, and α is the MOS current power index assumed to be between 1 and 2. By substituting (14) and (15) in (12), the ratio can be written as

$$\frac{tpl}{tph} = \frac{(un * Cox * (Wn_a/Ln_a)[(vdd - vtn)^{\alpha}])}{(up * Cox * (Wp_o/Lp_o)[(vdd - vtp)^{\alpha}])} \tag{16}$$

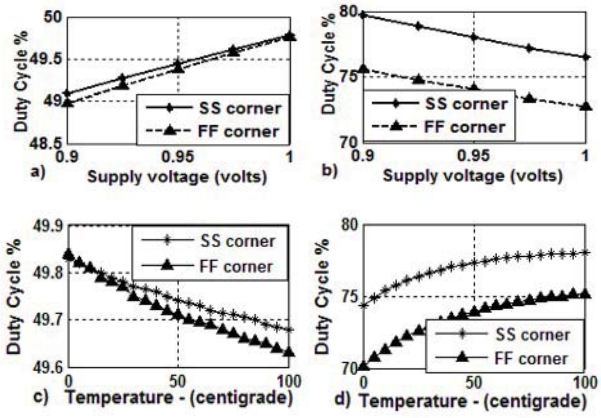

Fig. 6. Duty cycle variations versus supply voltage with (a) no mismatch and (b) mismatch. Duty cycle variations versus temperature with (c) no mismatch and (d) mismatch.

where (Wn_a/Ln_a) is the width-to-length ratio of the nMOS devices and is the same as the width-to-length ratio of the pMOS devices in the even stages, (Wp_o/Lp_o) is the width-to-length ratio of the pMOS devices of the odd inverter stages. From (16), the duty cycle spread expressed in (7) over FF and SS corners is amplified by the ratio of (Wn_a/Ln_a) to (Wp_o/Lp_o). The spread of the oscillation period (13) increases as the ratio of (Wn_a/Ln_a) to (Wp_o/Lp_o) increases. This increase, in turn, decreases the frequency spread expressed in (8) between FF and SS process corners.

The simulation of a seven-stage ring oscillator with the width-to-length ratio of the pMOS transistors for even stages set to be seven times larger than the transistors in odd stages is performed over SS and FF corners. As compared to a ring oscillator with equal width-to-length ratio for all transistors, a 4% higher duty cycle spread *(DS)* is achieved with the skewed sizing. Here, an improved VT reliability is achieved for mismatched ring oscillator with nonintersecting curves for SS and FF corners with a significantly reduced probability of flip-bit errors [3], [4]. The results are shown in Fig. 6(a) and (b) for the supply voltage variations from 0.9 to 1 V at 27 °C, and in Fig. 6(c) and (d), for the temperature variations from 0 °C to 100 °C at 0.95 V.

The results of Monte Carlo simulations of 200 mismatched ring oscillator samples at 0.95 V and 25 °C are shown in Fig. 7 where a standard deviation of 0.514% with a mean value of 75.3% is observed. The duty cycle spread between SS and FF corners and the corresponding standard deviation of the duty cycle is further enhanced by using dynamic control techniques, as described in Section IV.

III. Prior Relevant Work

A digitally controlled PWM with a current starved ring oscillator [14], [18] is tailored as the duty-cycle-based PUF primitive. The details of the architecture of the PWM are briefly provided in Section III-A. An analytical basis for modifying and using PWM as a PUF primitive is offered in Section III-B.

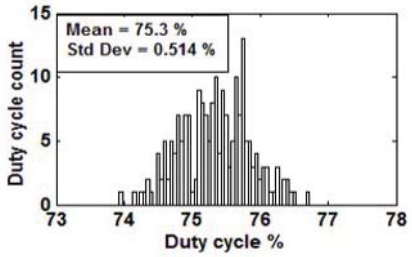

Fig. 7. Duty cycle histogram of the mismatched ring oscillator circuit output.

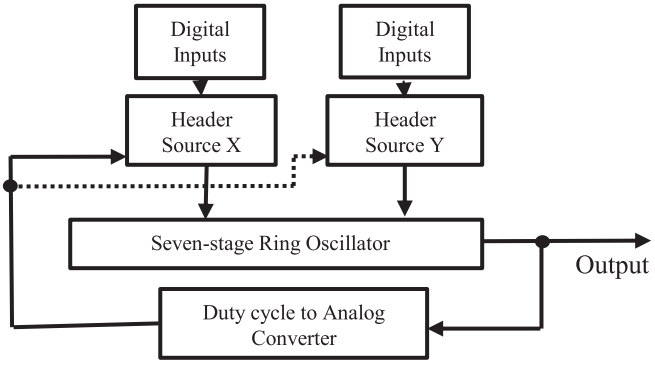

Fig. 8. Block diagram of the PWM.

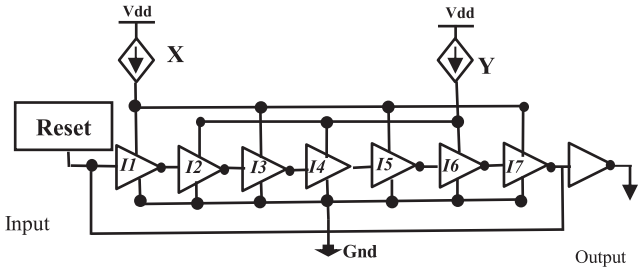

Fig. 9. Seven-stage current-controlled ring oscillator.

A. Digitally Controlled Pulsewidth Modulator

A digitally controlled PWM using a ring oscillator is shown in Fig. 8. A seven-stage ring oscillator, as shown in Fig. 9, is current starved with two header circuits X and Y. A digital block provides the control bits to program these headers for different output current values. The desired duty cycle and frequency are achieved by individually changing the currents through X or Y. The output of the ring oscillator is fed to the duty cycle to analog (D2A) converter block to generate a feedback signal which is used to control the current through X and Y to compensate for the changes due to PVT variations. The compensating current is provided by transistors $P_0, P_2, P_4, \ldots P_n$ as shown in header circuit in Fig. 10.

A seven-stage ring oscillator is used with X providing I_x current to odd inverter stages (*I1*, *I3*, *I5*, and *I7*) and Y providing I_y current to the even inverter stages (*I2*, *I4*, and *I6*). The relationship between the duty cycle and frequency as a function of I_x and I_y is [18]

$$D = 1/(1 + (i_x/i_y)) \tag{17}$$

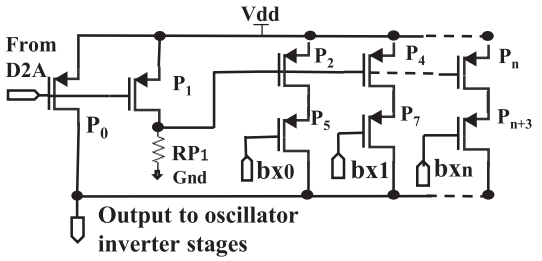

Fig. 10. Digitally controlled header current source.

where $i_x = I_x/I_{x5}$, $i_y = I_y/I_{y5}$ and I_{x5}, I_{y5} are the current passing through headers X and Y, respectively, to provide a 50% duty cycle. The frequency, F_{new}, of the PWM when the duty cycle D varies from 50% value can be written as

$$F_{\text{new}} = 2[(1 - D)F_0] \tag{18}$$

where F_0 is the frequency of the PWM when D is equal to 0.5. To maintain a constant frequency, the ratio of the source currents I_x to I_y is established for each value of duty cycle D as

$$I_y/I_x = D(1 - D). \tag{19}$$

The proposed digital control allows to maintain a constant ratio of source currents I_x and I_y to maintain a constant duty cycle.

B. Duty Cycle Sensitivity Analysis

The mathematical analysis of the sensitivity of the duty cycle with respect to i_x and i_y provides a basis to justify the utilization of the proposed circuit as a promising alternative to conventional PUFs. The partial derivative of the duty cycle D with respect to i_x and i_y is

$$\Delta D = \frac{1}{i_y(1 + (i_x/i_y))^2}\{(i_x/i_y)\Delta i_y - \Delta i_x\} \tag{20}$$

$$\Delta D = \frac{1}{i_x(1 + (i_y/i_x))^2}\{\Delta i_y - (i_y/i_x)\Delta i_x\} \tag{21}$$

where ΔD is the change in the duty cycle as a result of changes Δi_x and Δi_y in current i_x or i_y, respectively. The details of the derivation are offered in Appendix A.

From (20), if Δi_y is not altered, the change in the duty cycle ΔD is proportional to Δi_x scaled by a factor depending on the i_x/i_y ratio and the absolute value of i_y. The scaling factor has a maximum value of 1 when i_x/i_y is small as compared to 1 and i_y is close to 1. To achieve a small i_x/i_y when i_y is equal to 1, i_x has to be close to 0. Under these conditions, the changes in D are proportional to the change in i_x, $(-\Delta i_x)$. A small i_x/i_y implies that the duty cycle D is highly relative to 50% value. For the circuit shown in Fig. 8, the value of the current coming from X is a small fraction of the current coming from source Y to achieve a high duty cycle variability. A similar analysis of (21) leads to the conclusion that the current coming from Y is a small fraction of current coming from X to obtain high duty cycle variability.

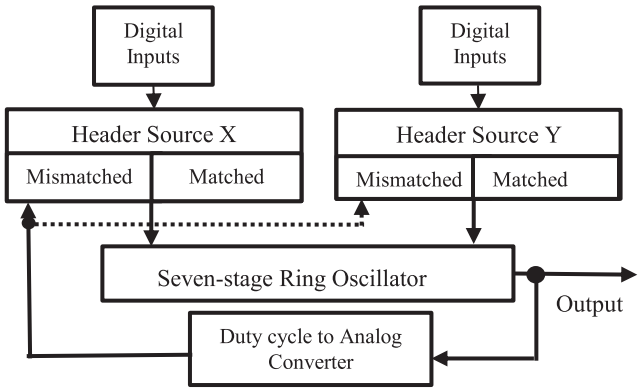

Fig. 11. Proposed duty cycle controlled PUF primitive.

IV. Proposed Duty-Cycle-Based PUF Primitive Circuit and Architecture

Following the guidelines established in Section III-B, the PWM shown in Fig. 8 is implemented as the proposed controlled and reconfigurable PUF primitive, as shown in Fig. 11. Headers X and Y consist of geometrically mismatched and matched branches. The mismatched and matched branches have transistors with different width-to-length ratios. The mismatched header branches for X and Y are turned ON in a mutually exclusive manner during the configuration and operation of the PUF. The circuit schematic of the header current source is shown in Fig. 12 for $(n+1)$ branches, where n is a positive integer. The circuit is designed and configured to achieve the following goals.

1) provide a uniform dynamic control of output current supplied to the odd and even inverter stages with digital control;
2) amplify the output current variation spread over FF and SS process corners;
3) achieve reliable current control operation over a wide range of mismatched circuit sizes.

The header current source shown in Fig. 10 is designed to provide a uniform dynamic control with a minimum current variation over FF and SS process corners, temperature, and supply voltage variations [14], [18]. For a PUF application, the circuit is designed to provide an amplified variation of the current at the source output. The details of the work to achieve goals 2) and 3) using the new current source shown in Fig. 12 are described in Sections IV-A–IV-C. The new circuit operates in a similar manner as the PWM with widely different output characteristics. The proposed PUF circuit can be dynamically configured to produce a wide range of random duty cycle values using the digital control and feedback signal from the D2A block. The PUF circuit is reliable under temperature and supply voltage variations. The details are explained in Sections IV-D–IV-F.

The details of the implementation of the challenge–response pair generation logic are shown in Fig. 13. The challenge is the selection of the multiplexer bits that are used to determine the pairs of PUF primitives for duty cycle comparison. The duty cycle comparison is accomplished with counters that generate response bits. The digital inputs of the header current are dedicated to control and configure the PUF as described in Section IV-F.

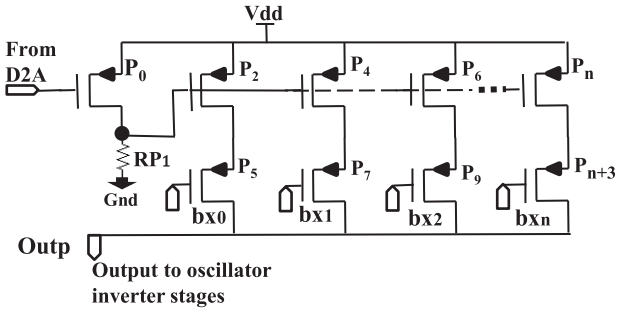

Fig. 12. Digitally controlled current source.

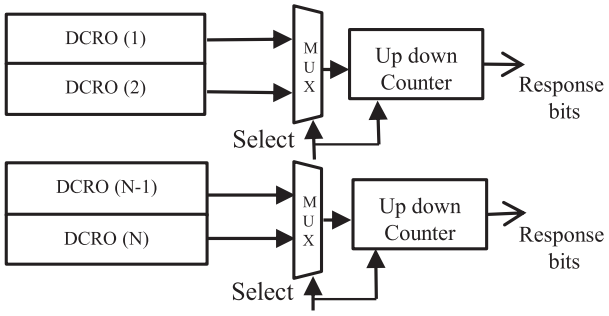

Fig. 13. Duty cycle controlled PUF challenge response blocks.

A. Header Current Source Variability Analysis

Detailed mathematical analysis to determine the conditions to enhance the entropy of the duty cycle under statistical variations in the device model parameters and circuit operating conditions is presented. In Fig. 12, transistors $P_5, P_7, P_9, \ldots, P_{n+3}$ operate in saturation region when digital inputs $bx0, \ldots bxn$ are turned ON. The transistors $P_2, P_4, P_6, \ldots, P_n$ are biased to operate in linear region using the transistor P_0, resistor RP1, and input signal from D2A. The total current I flowing through the output port *Outp* can be written as

$$I = I_0 + I_1 + I_2 + I_3 + \cdots + I_n \tag{22}$$

where $I_0, I_1, I_2, I_3 \ldots, I_n$ are the current flowing through transistors $P_5, P_7, P_9, \ldots, P_{n+3}$, respectively, when $bx0, bx1, bx2, \ldots, bxn$ are set to active. The total variation of current ΔI is the sum of the variation for each component in I as

$$\Delta I = \Delta I_0 + \Delta I_1 + \Delta I_2 + \Delta I_3 + \cdots + \Delta I_n \tag{23}$$

where ΔI_i is the total variation in current I_i and $0 < i < n$. The total variation of branch current ΔI_0 through transistors P_2 and P_5 is due to the combined effect of random variations of the model parameters and the source-to-gate voltage. Using the MOS square law model for device current, the total variation of ΔI_0 is expressed as

$$\Delta I_0 = [(-2\sqrt{(I_0)} - I_0)\Delta vth + 2(\Delta\beta/\beta)I_0] + [2\sqrt{(I_0)}\sqrt{\beta}\Delta vsg_{p5} + I_0\Delta vsg_{p2}] \tag{24}$$

where Δvth is the change in device threshold voltage, $\Delta\beta$ is the change in transconductance factor due to the device mobility, Δvsg_{p5} and Δvsg_{p2} are, respectively, the source-to-gate voltage on P_5 and P_2. The details of the derivation are provided in Appendix B.

From (24), the variation in ΔI_0 due to transistor process parameters, such as threshold voltage *vth* and mobility β variation can be written as

$$\Delta I_0(p) = [(-2\sqrt{(I_0)} - I_0)\Delta vth + 2(\Delta\beta/\beta)I_0]. \quad (25)$$

The variation in ΔI_0 due to the changes in the source–gate voltage Δvsg_{p5} and Δvsg_{p2} is

$$\Delta I_{0(vsg)} = [2\sqrt{(I_0)}\sqrt{\beta}\Delta vsg_{p5} + I_0 - \Delta vsg_{p2}]. \quad (26)$$

For identical header branches, the cumulative variation of the output current I, ΔI_n, for the header with *(n+1)* branches is

$$\Delta I_n = \sum_{i=0}^{n}[(-2\sqrt{(I_n)} - I_n)\Delta vth + 2(\Delta\beta/\beta)I_n] + \sum_{i=0}^{n}[2\sqrt{(I_0)}\sqrt{\beta}\Delta vsg_{p(n+3)} + I_n\Delta vsg_{p(n)}]. \quad (27)$$

B. Mismatched Current Source Analysis

Referring to current source in Fig. 12, (17), and (27), the variation of the source-to-gate voltage on transistor P_2 amplifies the current variation ΔI and, accordingly, the duty cycle variation at the output. The amplified current variation allows a method to develop a circuit with higher duty cycle variation over process corners and, correspondingly, the entropy of the duty cycle at the PUF output can be significantly increased.

Let us designate transistor P_2 in Fig. 11 as P_{2x} and P_{2y}, respectively, and the transistor P_5 as P_{5x} and P_{5y} for headers X and Y, as shown in Fig. 10. The width-to-length ratio of transistors P_{5x} and P_{5y} are mismatched to produce source-to-drain voltage mismatch. Under these conditions, the ratio of the current flowing through transistors P_{2x} and P_{2y} operating in linear region is

$$\frac{\mathrm{IP}_{2x}}{\mathrm{IP}_{2y}} = \frac{\left(\frac{vsg-vth}{vsd_y}\right)\left(\frac{1}{K}\right) - \left(\frac{1}{2K^2}\right)}{\left(\frac{vsg-vth}{vsd_y}\right) - 1/2} \quad (28)$$

where IP_{2x} and IP_{2y} are, respectively, the current flowing through transistors P_{2x} and P_{2y}, vsg is the gate-to-source voltage from D2A, vth is the threshold voltage, vsd_y is the source-to-drain voltage of transistor P_{2y}, vsd_x is the source-to-drain voltage of transistor P_{2x}, and $K = (vsd_y/vsd_x)$ is the mismatch factor. The details of the derivation are provided in Appendix C. For P_{2x} and P_{2y} operating in the linear region, i.e., $[(vsg - vth)/vsd_y] \geq 1$, the maximum value for (28) is

$$\mathrm{Max}\left|\frac{\mathrm{IP}_{2x}}{\mathrm{IP}_{2y}}\right| = \frac{\left(\frac{1}{K}\right) - \left(\frac{1}{2K^2}\right)}{0.5}. \quad (29)$$

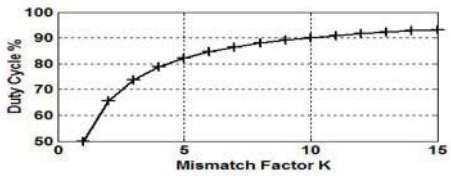

Fig. 14. Variation of duty cycle with source–drain mismatch factor K.

For large K, (29) reduces to $(2/K)$ and for small K, (29) can be approximated as $(1/K^2)$. Since the duty cycle has a reciprocal relationship with the ratio of the currents $(\mathrm{IP}_{2x}/\mathrm{IP}_{2y})$, the duty cycle varies quadratically for small K and linearly for large K, as observed from (21). For large K, duty cycle converges to the maximum value between 90% and 100%. Using (17) and (29), the amplification of the duty cycle with factor K is illustrated in Fig. 14.

C. Duty Cycle Spread Enhancement With Source–Gate Voltage

The upper and lower limits of the current ratio expressed in (28) under process corner conditions are determined by the upper and lower limits of the threshold voltage variations over the process corners, value of K, and source-to-gate voltage of transistors P_{2x} and P_{2y}. To achieve a high duty cycle spread over process corners, the difference of the ratio of currents expressed in (28) has to be maximized over SS and FF corners. Designating $(\mathrm{IP}_{2xf}/\mathrm{IP}_{2yf})$ as the ratio expressed in (28) under FF corner and $(\mathrm{IP}_{2xs}/\mathrm{IP}_{2ys})$ under SS corner, the conditions for maximizing the duty cycle spread is

$$\mathrm{DS} = \mathrm{Max}\left|\frac{\mathrm{IP}_{2xf}}{\mathrm{IP}_{2yf}} - \frac{\mathrm{IP}_{2xs}}{\mathrm{IP}_{2ys}}\right| \quad (30)$$

where DS represents the maximum duty cycle spread over FF and SS corners. After substituting (28) in (30) for FF and SS corners, the simplified result can be written as

$$\mathrm{DS} = \mathrm{Max}\left|\frac{\left(\frac{\mathrm{vsg}_f-\mathrm{vth}_f}{\mathrm{vsd}_{yf}}\right)\left(\frac{1}{K}\right) - \left(\frac{1}{2K^2}\right)}{\left(\frac{\mathrm{vsg}_f-\mathrm{vth}_f}{\mathrm{vsd}_{yf}}\right) - 0.5} - \frac{\left(\frac{\mathrm{vsg}_s-\mathrm{vth}_s}{\mathrm{vsd}_{ys}}\right)\left(\frac{1}{K}\right) - \left(\frac{1}{2K^2}\right)}{\left(\frac{\mathrm{vsg}_s-\mathrm{vth}_s}{\mathrm{vsd}_{ys}}\right) - 0.5}\right| \quad (31)$$

where the subscripts f and s refer to, respectively, FF and SS corners. Assuming that the source–drain voltage vsd_y is approximately kept constant under process variations, for a large value of K, an inspection of numerators and denominators in (31) shows that either a large value of vsg_f as compared to vth_f and simultaneously, a small value of vsg_s close to vth_s or vice versa, ensures that DS is maximized.

The impact on the changes in the duty cycle spread (DS) for high impact values of vsg_f and vsg_s is found using an analysis of (31) for various values of K. The results of circuit simulation with the corresponding values of vsg_f and vsg_s over SS and FF process corners are shown in Fig. 15. The theoretical results for various values of K, using (31), are shown

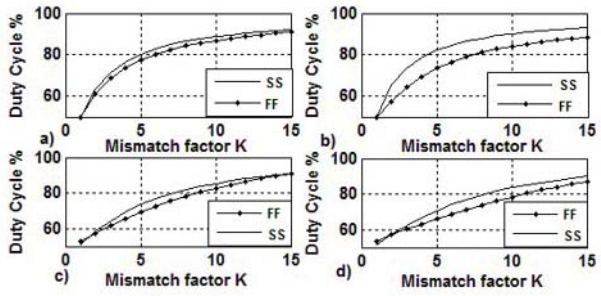

Fig. 15. Impact of the source-to-gate voltage vsg on the duty cycle spread (*DS*) for different mismatch factor *K* values. (a) Theory using (31)–low vsg impact. (b) Theory using (31)–high vsg impact. (c) Circuit simulation–low vsg impact. (d) Circuit simulation–high vsg impact.

in Fig. 15(a) and (b). The simulation results for various values of the mismatch factor *K* are shown in Fig. 15(c) and (d). The duty cycle spread (DS) between SS and FF process corners is amplified from 4% to 10% with the appropriate selection of the source-to-gate voltage vsg for the headers transistors P_{2x} and P_{2y}, and the source-to-drain voltage mismatch factor *K*.

D. Proposed PUF Environmental Stability Enhancement

To guatantee a reliable PUF operation, the duty cycle of the PUF under SS and FF process conditions should not overlap over a wide temperature and voltage range, and stay distinctly separated to avoid a flip-bit error [3], [4]. To simplify the analysis, two parameters are defined from (31) as *G* and *H* as

$$G = \left(\frac{\text{vsg}_f - \text{vth}_f}{\text{vsd}_{yf}}\right) \tag{32}$$

$$H = \left(\frac{\text{vsg}_s - \text{vth}_s}{\text{vsd}_{ys}}\right). \tag{33}$$

Assuming that vsd_{yf} are vsd_{ys} are approximately equal over process conditions, the values of *G* and *H* can be determined by the numerator by carefully selecting an appropriate value of *K*. The value of *K* is chosen to guarantee that *G* and *H* are greater than one and have significantly different values. The source-to-gate voltages vsg_f and vsg_s in (32) and (33) are determined to ensure that the duty cycle is a monotonic function and has different values for each process corner (SS, FF), resulting to provide a wide duty cycle spread over the operating temperature and voltage range.

E. Proposed PUF Simulation Results

Following the guidelines in Sections III-B and IV-A–IV-D, the proposed PUF circuit is implemented with 22-nm-LP CMOS PTM [19]. Extensive circuit simulations of the proposed PUF over SS and FF corners are performed to demonstrate the feasibility and reliability under temperature and supply voltage variations. The results are shown in Fig. 16(a) for supply voltage of 0.95 V and at a temperature between 0 °C–100 °C, and in Fig. 16(b), over supply voltage between 0.9–1 V at a temperature of 25 °C. The duty cycle spread of the proposed PUF is 10% under SS and FF corners over the specified temperature and voltage ranges. The increased

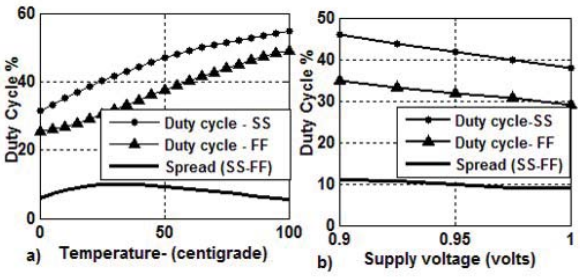

Fig. 16. FF and SS corner simulations of the PUF circuit under varying (a) temperature and (b) supply voltage.

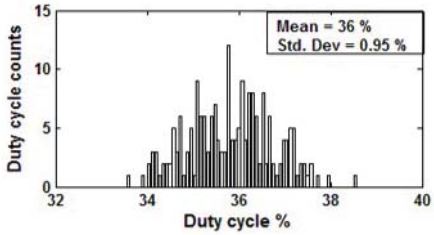

Fig. 17. Duty cycle histogram of PUF circuit output.

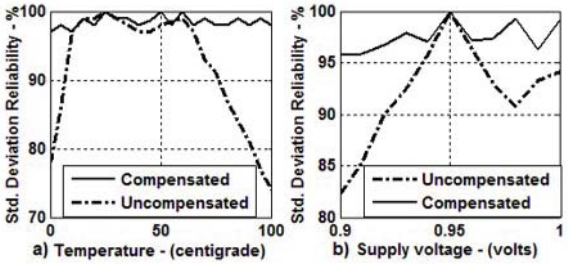

Fig. 18. Standard deviation reliability of the duty cycle with (a) temperature compensation and (b) supply voltage compensation.

duty cycle spread as compared to that of the mismatched ring oscillator of 4%, in Section II-D, ensures increased entropy and a reduced probability of flip-bit errors [3], [4], thus improving the PUF reliability. The results of the Monte Carlo simulations at 0.95 V and 25 °C are illustrated in Fig. 17. A standard deviation of 0.95% with a mean value of 36% is observed. The standard deviation is approximately two times greater than a mismatched ring oscillator without feedback, as shown in Fig. 7.

Utilizing a digital compensation scheme, the proposed PUF circuit is configured to provide a uniform and stable standard deviation over temperature and supply voltage variations. The digital inputs are configured to control the current ratio of the header current sources *X* and *Y*. Monte Carlo circuit simulations of 100 samples are performed between 0 °C–100 °C at 0.95 V and 0.9–1 V at 25 °C, respectively. The reliability of the standard deviation of duty cycle is compared with the reference value of 100% at nominal conditions of 0.95-V supply voltage and 25 °C temperature, as shown in Fig. 18.

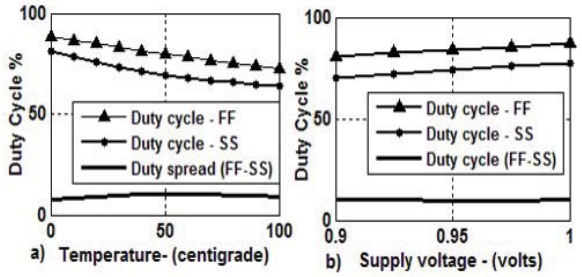

Fig. 19. Corner simulation results of the reconfigured PUF circuit under varying (a) temperature and (b) supply voltage.

F. Reconfigurable PUF Operation

The proposed PUF can be used as a reconfigurable PUF [16]. A new configuration of the PUF is formed when the header current sources X and Y for mismatched and matched branches of PUF shown in Fig. 11 are swapped with digital control. The duty cycle response under SS and FF corners for a supply voltage of 0.95 V over a temperature range of 0 °C–100 °C is shown in Fig. 19(a) and supply voltage variations between 0.9–1 V at a temperature of 25 °C is shown in Fig. 19(b). As compared to the simulation results of an existing configuration (i.e., shown in Fig. 16), when the FF and SS corners are swapped, the reconfigured PUF generates a different response output bit pattern.

The duty cycle spread of the reconfigured PUF is about 10% between SS and FF corners over the specified temperature and supply voltage ranges. The increased duty cycle spread as compared to the mismatched ring oscillator of 4%, in Section II-D, ensures an increased entropy level and a reduced probability of flip-bit errors [3], [4], thus improving the PUF reliability.

The interconfiguration PUF metric (I_C) defined in [16] to compare different PUF configurations is defined as

$$I_C = \frac{1}{c(c-1)}\left[\sum_{s=1}^{s=(c-1)}\sum_{t=0,s\neq t}^{t=(c-1)}\frac{\text{Hammd}(U_s\ U_t)}{(r-1)}\right]\times 100 \quad (34)$$

where c is the number of configurations, r is the number of response bits, and Hammd (U_s U_t) is the Hamming distance between configurations s and t. Monte Carlo circuit simulations of two PUF configurations producing 200 response bits at nominal conditions of 0.95 V and 25 °C are performed. The corresponding I_C value determined with (34) is 40%.

V. PUF Qualitative Characteristics and Measures

Extensive Monte Carlo statistical simulations are performed to characterize statistical models and determine the qualitative figures of merits of uniqueness and reliability.

A. Uniqueness

Uniqueness R of a PUF circuit is defined as the average interdie Hamming distance measured as a percentage value over n instances as [22]

$$R = \frac{2}{n(n-1)}\left[\sum_{x=1}^{x=(n-1)}\sum_{y=(x+1)}^{y=n}\frac{\text{Hammd}(U_x\ U_y)}{\text{nb}}\right]\times 100 \quad (35)$$

where n is the number of PUF instances, U_x and U_y are the output response vectors for PUF instance numbers x and y, Hammd is the Hamming distance function, and nb is the number of PUF response bits. Monte Carlo simulations on $n = 12$ PUF instances at nominal supply voltage of 0.95 V, temperature of 25 °C, and nb = 200 response bits achieve a uniqueness value of 49.3%.

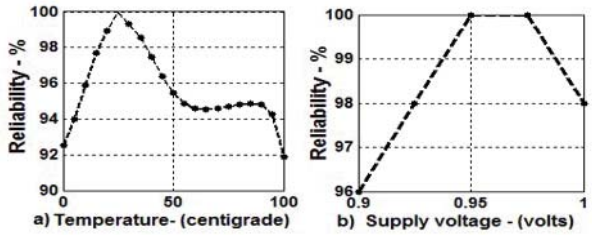

Fig. 20. (a) Temperature reliability. (b) Supply voltage reliability.

B. Reliability

The reliability under temperature and voltage variations is also analytically determined by estimating the bit error rate (BER) of the output response bit pattern. The BER and percentage reliability Rb can be written [22] as

$$\text{Rb} = 1 - \text{BER} = 1 - \left[\frac{1}{m}\sum_{y=1}^{y=m}\frac{\text{Hammd}(U_x\ U_y)}{\text{nb}}\right]\times 100 \quad (36)$$

where U_x is the response of the PUF under nominal operating conditions, m is the number of times the challenge is repeated on an instance of the PUF under conditions other than nominal, U_{xy} is the response of PUF under operating conditions other than nominal, Hammd is the Hamming distance function, and nb is the number of bits in the response. Monte Carlo statistical simulations are performed on the proposed PUF circuit over a temperature range of 0 °C–100 °C with 5 °C increments at 0.95-V supply voltage for nb = 200 bit response with the same challenge to determine the temperature reliability. The results are illustrated in Fig. 20(a) where the reliability is greater than 92% over an operating temperature range of 0 °C–100 °C. Supply voltage reliability is determined by performing the Monte Carlo simulation at 25 °C temperature and at a voltage range of 0.9–1 V with 0.025-V increments for nb = 200 bit response with the same challenge. The results are shown in Fig. 20(b) where the supply voltage reliability is greater than 96% over the operating voltage range.

VI. PUF Comparisons

A comparison of the uniqueness, reliability, power consumption, and circuit area of the proposed PUF with other state-of-the-art PUF implementations is presented in Table I. In the absence of the actual implementation of a test chip, the layout area estimate of the proposed PUF is based on the active area of the devices shown in Fig. 11 with an added

TABLE I

PROPOSED PUF COMPARISONS R = UNIQUENESS %AGE, TRB = TEMPERATURE RELIABILITY %AGE, VRB = VOLTAGE RELIABILITY %AGE, P = POWER IN (μW), P_n = POWER NORMALIZED TO 22 nm SCALING IN (μW), A = AREA IN (μM^2), A_n = AREA NORMALIZED TO 22 nm SCALING IN (μM^2), TE = CMOS TECHNOLOGY NODE IN NANOMETER, **TW** = THIS WORK

Design	R	TRB[0]	VRB[0]	$P/(P_n)$	$A/(A_n)$	Te
[23]	50.42	98.25	97.22	32.3/(3.7)	250/(28.6)	65
[24]	51	85	92	134/(32)	N/A	45
[25]	50.11	97.8	97.8	N/A	825/(12.3)	180
[26]	49.5	97.2	N/A	N/A	58.8/(6.73)	65
[3]	46.15	99.5[1]	99.5[1]	N/A	N/A	90
[15]	49.8[2]	95	N/A	N/A	N/A	40
TW	49.3	92	96	3.75[3]	15[4]	22

[0] Reliability conditions for temperature and voltage variations are different for each case. Worst case values reported unless otherwise noted.
[1] Average reliability value over 128 instances under temperature range of -20°C-120°C and supply voltage range of 1.2V-1.08V.
[2] Estimated from data plot provided in the corresponding work.
[3] Power results for **TW** under nominal operating conditions at 27°C, 0.95V, and FF process corner at 32MHz.
[4] Estimated area based on the circuit shown in Fig. 11 with an added overhead of 3X allocated for interconnects and placement [27].
N/A=Not available

overhead of 3× allocated for interconnects and placement of circuit blocks in a typical IC layout [27]. Accordingly, the estimated area is 15 μM^2.

The power consumption of the proposed PUF is determined based on the average current consumption that is determined with transistor-level simulations represented in Fig. 11. The estimated power consumption is 3.75 μW. Note that the estimated power consumption and area for each design in Table I are ideally-scaled to 22-nm CMOS technology to provide a fair comparison [28]. The proposed design provides reliable operation over a wide range of temperatures and supply voltages.

VII. CONCLUSION

A duty-cycle-based controlled and reconfigurable PUF primitive is proposed and validated. The proposed PUF provides a stable and reliable operation with a high entropy over a wide range of duty cycles under VT variations. The proposed feedback control provides a capability to enhance the duty cycle entropy over process parameter variations. The feedback loop incorporates a small number of logic blocks, a duty cycle to voltage converter, and a self-bias generation circuit, enabling fast response and stable operation. The current-starved inverter scheme provides a precise control of the circuit duty cycle by utilizing the digital inputs and enabling controllability and reconfigurability features. The PUF can also be adapted to operate at different frequencies and duty cycle values. In addition, the digital inputs potentially provide the capability to calibrate and tune the PUF primitive postimplementation and during testing.

The proposed circuit operates at a low frequency with a maximum frequency of 32 MHz with a power consumption of 3.75μW. The layout foot print is estimated to be in the order of 15 μM^2 which can be uniformly placed as a macrocell on a die for cryptography and security applications. The output has a low frequency of less than 32 MHz, and therefore, is measurable with low-frequency, low-cost, and low-resolution instrumentation.

APPENDIX A
SENSITIVITY ANALYSIS OF THE DUTY CYCLE

The details of the sensitivity analysis of the duty cycle variation with respect to header source currents i_x and i_y defined in Section III are provided in this Appendix. Referring to (17), the duty cycle is

$$D = 1/(1 + (i_x/i_y)) = \frac{i_y}{(i_x + i_y)}. \tag{37}$$

Taking the partial derivative of (37) with respect to i_y gives

$$\frac{\delta D}{\delta i_y} = \frac{i_x}{(i_x + i_y)^2}. \tag{38}$$

After rearranging the terms and substituting $\Delta D_y = \delta D$ and $\Delta i_y = \delta i_y$, ΔD_y can be written as

$$\Delta D_y = \left(\frac{i_x}{(i_x + i_y)^2}\right) \Delta i_y. \tag{39}$$

Taking the partial derivative of (37) with respect to i_x gives

$$\Delta D_x = \left(\frac{-i_y}{(i_x + i_y)^2}\right) \Delta i_x. \tag{40}$$

Combining (39) and (40) to determine the total variation, ΔD can be written as

$$\Delta D = \left(\frac{i_x}{(i_x + i_y)^2}\right) \Delta i_y - \frac{i_y}{(i_x + i_y)^2} \Delta i_x \tag{41}$$

$$\Delta D = \frac{1}{(i_x + i_y)^2} (i_x \Delta i_y - i_y \Delta i_x). \tag{42}$$

After factoring i_x in (42), ΔD becomes

$$\Delta D = \frac{1}{i_x (1 + (i_y/i_x))^2} \{\Delta i_y - (i_y/i_x) \Delta i_x\}. \tag{43}$$

Additionally, after factoring i_y in (42), ΔD can be written as

$$\Delta D = \frac{1}{i_y (1 + (i_x/i_y))^2} \{(i_x/i_y) \Delta i_y - \Delta i_x\}. \tag{44}$$

APPENDIX B
SOURCE–GATE VOLTAGE IMPACT ON CURRENT VARIABILITY

The impact of source-to-gate voltage to amplify the variation of the header source currents due to process parameter variations is described in this Appendix. The transistor P_5 shown in Fig. 12 is biased in the saturation region. The current I_{p5} through P_5 is approximated using the MOS square law as

$$I_{p5} = \beta_0 (\text{vsg}_0 - \text{vth}_0)^2 \tag{45}$$

where β_0 is the nominal mobility transconductance factor for MOS transistors P_5 and vsg_0 is the source-to-gate voltage. Taking the partial derivatives of (45) with respect to the

transconductance factors β_0, threshold voltage vth_0, and gate-to-source voltage vsg_0, ΔI_{p5} can be written as

$$\begin{aligned}\Delta I_{p5} = &-2\beta_0(\text{vsg}_0 - \text{vth}_0)\Delta\text{vth}_0 \\ &+ \Delta\beta_0(\text{vsg}_0 - \text{vth}_0)^2 \\ &+ 2\beta_0(\text{vsg}_0 - \text{vth}_0)\Delta\text{vsg}_0. \end{aligned} \tag{46}$$

Here, P_2 is operating in linear region; ignoring the square term for small value of source-to-drain voltage, the current I_{p2} through P_2 can be approximated as

$$I_{p2} = \beta_3(\text{vsg}_3 - \text{vth}_3)\text{vsd} \tag{47}$$

where vsg_3 is the source-to-gate voltage, vth_3 is the threshold voltage, and vsd is the source-to-drain voltage. Ignoring the small changes in vsd and taking the partial differentials of I_{p2} with respect to β_3 and vth_3, ΔI_{p2} can be written as

$$\begin{aligned}\Delta I_{p2} = &-\beta_3(\text{vsg}_3 - \text{vth}_3)\Delta\text{vth}_3 \\ &+ \Delta\beta_3(\text{vsg}_3 - \text{vth}_3) \\ &+ \beta_3(\text{vsg}_3 - \text{vth}_3)\Delta\text{vsg}_3. \end{aligned} \tag{48}$$

Assuming that β_0 and β_3 are equal to β and threshold voltages vth_0 and vth_3 are equal to vth, substituting β and vth in (45), (46), (47), and (48) results in

$$\begin{aligned}\Delta I_{p5} = &-2\sqrt{(I_{p5})}\Delta\text{vth} + (\Delta\beta/\beta)I_{p5} \\ &+ 2\sqrt{(I_{p5})}\sqrt{\beta}\Delta\text{vsg}_0. \end{aligned} \tag{49}$$

$$\Delta I_{p2} = I_{p2}(\Delta\beta/\beta) - \Delta\text{vth} + \Delta\text{vsg}_3). \tag{50}$$

Since I_{p2} is the same as I_{p5} and the total variation in I_0 is the combined net effect of the variations through series connected P_2 and P_5, replacing I_{p2} and I_{p5} with I_0 on the right-hand side of (50), adding (49) and (50), and designating the total variation as ΔI_0 in I_0 results in

$$\begin{aligned}\Delta I_0 = &[(-2\sqrt{(I_0)} - I_0)\Delta\text{vth} + 2(\Delta\beta/\beta)I_0 \\ &+[2\sqrt{(I_0)}\sqrt{\beta}\Delta\text{vsg}_{p5} + I_0\Delta\text{vsg}_{p2}] \end{aligned} \tag{51}$$

where Δvsg_3 and Δvsg_0 are replaced with Δvsg_{p2} and Δvsg_{p5}, respectively.

APPENDIX C
SOURCE–DRAIN VOLTAGE MISMATCH

Mathematical analysis of the ratio of the header currents over SS and FF process corners by using skewed width-to-length ratio for the header sources is presented in this Appendix. The source-to-drain voltage mismatch is obtained by using skewed transistors with digital control inputs in matched and mismatched current source branches.

Referring to P_2 in Fig. 12 and analyzing the current changes in P_2 and P_5 due to the source-to-gate voltage of transistor P_2, the current through P_2 can be expressed in the linear region as

$$\text{IP}_2 = \beta_2(\text{vsg}_2 - \text{vth}_2)\text{vsd}_2 - \beta_2\frac{\text{vsd}_2^2}{2} \tag{52}$$

where IP_2 is the current through P_2, β_2 is the transconductance mobility parameter of P_2, vth_2 is the threshold voltage of P_2, vsg_2 is the source-to-gate voltage of P_2, and vsd_2 is the source-to-drain voltage of P_2.

Assuming that the transistors used both in the headers X and Y have the same threshold voltage, mobility, width, and length, the current through P_2, as shown in Fig. 12, for the headers X and Y, respectively, is

$$\text{IP}_{2x} = \beta(\text{vsg}_x - \text{vth})\text{vsd}_x - \beta\frac{\text{vsd}_x^2}{2} \tag{53}$$

$$\text{IP}_{2y} = \beta(\text{vsg}_y - \text{vth})\text{vsd}_y - \beta\frac{\text{vsd}_y^2}{2}. \tag{54}$$

where IP_{2x} and IP_{2y} refer to current through X and Y, respectively. For the same source-to-gate voltage applied to both of the current sources X and Y from the D2A converter, then $vsg_x = vsg_y$ can be substituted with vsg. If the transistor P_2 in Fig. 12, designated as P_{2x} and P_{2y} for headers X and Y, respectively, have a mismatched width-to-length ratio, the corresponding source-to-drain voltages vsd_x and vsd_y will be mismatched. The relationship between voltages vsd_x and vsd_y can be expressed as $\text{vsd}_x n = (1/K)\text{vsd}_y$, where K depends on the width-to-length mismatch ratio of the transistors P_{2x} and P_{2y}. The ratio of (53) and (54) can be expressed as

$$\frac{\text{IP}_{2x}}{\text{IP}_{2y}} = \frac{(\text{vsg} - \text{vth})\left(\frac{1}{K}\text{vsd}_y\right) - \left(\frac{1}{K^2}\right)\text{vsd}_y^2/2}{(\text{vsg} - \text{vth})\text{vsd}_y - \text{vsd}_y^2/2}. \tag{55}$$

After rearranging the terms in (55), the ratio becomes

$$\frac{\text{IP}_{2x}}{\text{IP}_{2y}} = \frac{\left(\frac{\text{vsg}-\text{vth}}{\text{vsd}_y}\right)\left(\frac{1}{K}\right) - \left(\frac{1}{2K^2}\right)}{\left(\frac{\text{vsg}-\text{vth}}{\text{vsd}_y}\right) - 1/2}. \tag{56}$$

REFERENCES

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[2] R. J. Anderson and M. G. Kuhn, "Low cost attacks on tamper resistant devices," in *Proc. 5th Int. Workshop Secur. Protocols*, Apr. 1997, pp. 125–136.

[3] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf.*, Jun. 2007, pp. 9–14.

[4] C. Herder, M.-D. Yu, F. Koushanfar, and S, Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[5] D. Blaauw, K. Chopra, A. Srivastava, and L. Scheffer, "Statistical timing analysis: From basic principles to state of the art," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 27, no. 4, pp. 589–607, Apr. 2008.

[6] M. H. Abu-Rahma and M. Anis, "Variability in VLSI circuits: Sources and design considerations," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2007, pp. 3215–3218.

[7] M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*. New York, NY, USA: Springer-Verlag, 2011.

[8] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Techniques for design and implementation of secure reconfigurable PUFs," *ACM Trans. Reconfigurable Technol. Syst.*, vol. 2, no. 1, Mar. 2009, Art. no. 5.

[9] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, Oct. 2010, pp. 237–249.

[10] G. Kömürcü, A. E. Pusane, and G. Dündar, "Dynamic programming based grouping method for RO-PUFs," in *Proc. 9th Conf. Ph.D. Res. Microelectron. Electron. (PRIME)*, Jun. 2013, pp. 329–332.

[11] C.-E. D. Yin and G. Qu, "LISA: Maximizing RO PUF's secret extraction," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2010, pp. 100–105.

[12] B. Gassend, M. Van Dijk, D. Clarke, D. Torlak, S. Devadas, and P. Devadas, "Controlled physical random functions and applications," *ACM Trans. Inf. System Secur.*, vol. 10, no. 4, Jan. 2008, Art. no. 4.

[13] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1327–1340, Oct. 2017.
[14] S. Köse, I. Vaisband, and E. G. Friedman, "Digitally controlled wide range pulse width modulator for on-chip power supplies," in *Proc. IEEE Symp. Circuits Syst. (ISCAS)*, May 2013, pp. 2251–2254.
[15] J. Augustin and M. L. Lopez-Vallejo, "A temperature-independent PUF with a configurable duty cycle of CMOS ring oscillators," in *Proc. IEEE Symp. Circuits Syst. (ISCAS)*, May 2016, pp. 2471–2474.
[16] X. Xin, J.-P. Kaps, and K. Gaj, "A configurable ring-oscillator-based PUF for Xilinx FPGAs," in *Proc. Euromicro Conf. Digit. Syst. Design (DSD)*, Sep. 2011, pp. 651–657.
[17] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, P. Sundaravadivel, and J. Singh, "Reconfigurable robust hybrid oscillator arbiter PUF for IoT security based on DL-FET," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Jul. 2017, pp. 665–670.
[18] I. Vaisband, M. Azhar, S. Köse, and E. G. Friedman, "Digitally controlled pulse width modulator for on-chip power management," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 22, no. 12, pp. 2527–2534, Dec. 2014.
[19] NIMO Group and Arizona State University. *Predictive Technology Model (PTM)*. Accessed: Nov. 15, 2008. [Online]. Available: http://ptm.asu.edu
[20] M. Mustapa, M. Niamat, M. Alam, and T. Killian, "Frequency uniqueness in ring oscillator physical unclonable functions on FPGAs," in *Proc. IEEE 56th Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2013, pp. 465–468.
[21] Y. Cao, X. Huang, D. Sylvester, T.-J. King, and C. Hu, "Impact of on-chip interconnect frequency-dependent R(f)L(f) on digital and RF design," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 1, pp. 158–162, Jan. 2005.
[22] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *J. Cryptol.*, vol. 24, no. 2, pp. 375–397, 2011.
[23] Y. Cao, L. Zhang, C.-H. Chang, and S. Chen, "A low-power hybrid RO PUF with improved thermal stability for lightweight applications," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 7, pp. 1143–1147, Jul. 2015.
[24] R. Kumar, V. C. Patil, and S. Kundu, "Design of unique and reliable physically unclonable functions based on current starved inverter chain," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Jul. 2011, pp. 224–229.
[25] M. Wan, Z. He, S. Han, K. Dai, and X. Zou, "An invasive-attack-resistant PUF based on switched-capacitor circuit," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 8, pp. 2024–2034, Aug. 2015.
[26] R. Maes, V. Rozic, I. Verbauwhede, P. Koeberl, E. van der Sluis, and V. van der Leest, "Experimental evaluation of physically unclonable functions in 65 nm CMOS," in *Proc. ESSCIRC*, Sep. 2012, pp. 486–489.
[27] P. Saxena, R. Shelar, and S. Sapatnekar, *Routing Congestion in VLSI Circuits: Estimation and Optimization*, New York, NY, USA: Springer-Verlag, 2007.
[28] E. Salman and E. G. Friedman, *High Performance Integrated Circuit Design*. New York, NY, USA: McGraw-Hill, 2012

Mahmood J. Azhar (M'84) received the M.S.E.E degree in electrical engineering from the University of Wisconsin–Madison, Madison, WI, USA, in 1984. He is currently working toward the Ph.D. degree in electrical engineering at the University of South Florida, Tampa, FL, USA.

During 1984 and 1985, he was a Component Engineer with the Custom Products Group, Intel Corporation, Chandler, AZ, USA. From 1986 to 1987, he was a Member Technical Staff with the CMOS Gate Array Design Automation Group, GTE Microcircuits, Tempe, AZ, USA. From 1987 to 1994, he was a Senior Engineer with the Custom Products and Analog Mix-Signal Design Division, Semiconductors Group, Motorola Inc., in Chandler, AZ, USA and Tempe, AZ, USA. From 1994 to 2001, he was a Staff Engineer with Communications Group, Paging products Group, Motorola Inc., Boynton Beach, FL, USA. From 2001 to 2007, he was a Principal Staff Engineer with Research Labs, RFIC Labs Division, Motorola Inc., Plantation, FL, USA. From 2008 to 2009, he was a Lead Engineer with Cadence Design Systems, Melbourne, FL, USA. In 2015, he was a Consultant with Qualcomm, Raleigh, NC, USA, where he was a CPU Custom Circuit Design Methodology Engineer. He is currently an Active Research and Teaching Assistant at the Department of Electrical Engineering, University of South Florida. His current research interests include the design of high performance integrated circuits.

Fathi Amsaad (M'12) was born in Benghazi, Libya, in 1980. He received the B.Sc. degree in computer science from the University of Benghazi, Benghazi, Libya, in 2001, the dual M.Sc. degrees in computer science and computer engineering from the University of Bridgeport, Bridgeport, CT, USA, in 2012, and the Ph.D. degree in engineering science from the Electrical Engineering and Computer Science (EECS) Department, University of Toledo, Toledo, OH, USA, in 2017, with a focus on computer science and engineering.

He was a Teaching and Research Graduate Assistant with the EECS and Engineering Technology (ET) Departments, University of Toledo. In 2014, he joined the Electronic and Computer ET Department, College of Technology Architecture and Applied Engineering, Bowling Green State University, Bowling Green, OH, USA, as an Adjunct Instructor. He was a Project Adviser for several groups of senior undergraduate students. He was a Full-Time Visiting Instructor with the Department of Computer Science and Engineering, University of South Florida, Tampa, FL, USA. He has authored or/and coauthored more than 25 peer reviewed papers. His current research interests include cyber security and cyber-physical systems with special interests in hardware oriented security and trust, embodied systems design, ASICs/FPGAs security, digital/VLSI systems testing, fault tolerance hardware, detection of hardware Trojans, network security, and security of smart grids.

Dr. Amsaad is an Active Member and serves as a reviewer for ACM and IEEE conferences. He was a recipient of the IEEE Best Graduate Student Award in 2016, by the IEEE region 4 and the College of Engineering, University of Toledo.

Selçuk Köse (S'10–M'12) received the B.S. degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2006 and the M.S. and Ph.D. degrees in electrical engineering from the University of Rochester, Rochester, NY, USA, in 2008 and 2012, respectively.

He was with TUBITAK, Ankara, Intel Corporation, Santa Clara, CA, USA, and Freescale Semiconductor, Tempe, AZ, USA. He is currently an Assistant Professor at the Department of Electrical Engineering, University of South Florida, Tampa, FL, USA. His current research interests include integrated voltage regulation, 3-D integration, hardware security, and green computing.

Dr. Köse was a recipient of the NSF CAREER Award, the Cisco Research Award, the USF College of Engineering Outstanding Junior Researcher Award, and the USF Outstanding Faculty Award. He is an Associate Editor of the *Journal of Circuits, Systems, and Computers* and *Microelectronics Journal*. He has served on the Technical Program and Organization Committees of various conferences.