Process, Voltage, and Temperature-stable Adaptive Duty Cycle based PUF

Mahmood J. Azhar
Electrical Engineering Department
University of South Florida
Tampa, Florida, USA
mazhar@mail.usf.edu

Selçuk Köse
Electrical Engineering Department
University of South Florida
Tampa, Florida, USA
kose@usf.edu

***Abstract*—A duty cycle controlled pulse width modulator (PWM) is designed and tailored to provide PVT (process, voltage and temperature) stable, duty cycle comparison based PUF primitive for security applications. The proposed circuit uses a current starved ring oscillator whose duty cycle can be controlled over a wide range of 20%-90%. This proposed PVT compensated circuit provides a stable and uniform duty cycle with a worst case error between 1%-2% over an operating temperature range of 0°C-100°C, supply voltage range of 0.95 V-1.05 V, and fast fast (FF) and slow slow (SS) manufacturing process conditions. This proposed reliable and controlled PUF primitive is configurable to accept controlled random digital inputs to provide random and configurable duty cycle output values over a wide range.**

***Index Terms*—Physical unclonable function, Hardware security, Pulse width modulator, Ring oscillator**

I. Introduction

Switching DC-DC voltage regulators are widely used for on-chip voltage regulation with high power conversion efficiency [1], [2]. An important property of switching DC-DC regulators is to control the duty cycle of input switching signal to scale the DC output [3]. A PVT stable pulse width modulator (PWM) based on a current starved ring oscillator is proposed in [4–6], to provide the duty cycle control function for a switching DC-DC regulators [2], [7–13].

Adding security protocols to voltage regulation function is an important benefit that can used to provide a capability to counter side-channel power analysis attacks [14–20]. A duty cycle controlled PWM with the capability to use random inputs is proposed to develop a controlled PUF primitive for security applications. Controlled PUF primitives are versatile components of programmable security applications as discussed in [21], [22]. In a conventional ring oscillator PUF [23–26], frequency comparison of a set of matched ring oscillators is used as a criteria to generate an output response bit.

PUF circuits use the underlying manufacturing process variations to produce a set of random frequencies [26]. The frequency of a ring oscillator is highly sensitive to temperature, voltage variations, and device aging, potentially reducing the PUF reliability [27]. Although error correction schemes can be used to mitigate the impact of variations, error correction increases the cost and vulnerability to the PUF implementations [26], [29]. Post processing of PUF response data and error correction schemes are proposed in [28–31]. The cost of error correction can be considerably reduced with a PVT stable PUF circuit. A PVT stable and reliable PUF circuit has previously been proposed using circuit compensation methods [32], [33].

A temperature stable PUF primitive based on ring oscillator duty cycle comparisons has also recently been proposed [34]. The proposed PUF uses delay-mismatched inverter stages exploiting width-to-length mismatch among ring oscillator stages. This mismatch produces a different duty cycle at each inverter stage. This PUF therefore consists of a fifteen stage ring oscillator to produce distinct duty cycles. This PUF also lacks the capability of a controlled PUF. Alternatively the PUF primitive proposed in this paper uses a current starved ring oscillator with seven stages to introduce delay-mismatched inverters that produce distinct duty cycles at the output of each stage [5]. A PVT stable, low power operation, and reliable PUF primitive is realized using feedback techniques. Stable threshold values can be used to distinguish between duty cycles to differentiate between wrong and valid comparison conditions. In addition to the manufacturing process variations to provide random values that conventional PUFs rely on, the proposed PUF also houses digitally controlled current sources that can be configured to provide a random challenge to produce a random set of duty cycles over a wide range for response bit generation.

The rest of the paper is organized as follows. In Section II, the basis for duty cycle based PUF primitive is explored. The features of the tailored PWM and the adaptation of the PWM as a variable duty cycle based PUF primitive is reviewed in Section III. In Section IV, the details of proposed PUF primitive and the reliability over PVT variations are discussed with Monte Carlo circuit simulations and at different corner conditions. The details of the Monte Carlo simulation based statistical reliability analysis of the proposed PUF are offered in Section V. Conclusions are provided in Section VI.

II. Duty Cycle based PUF

A typical ring oscillator with N integral stages has N output nodes available along the chain. With balanced rise

This work is supported in part by the National Science Foundation CAREER Award under Grant CCF-1350451, by the National Science Foundation Award under Grant CNS-1715286, and by a Cisco Systems Research Award.

978-1-5386-4881-0/18/$31.00 ©2018 IEEE

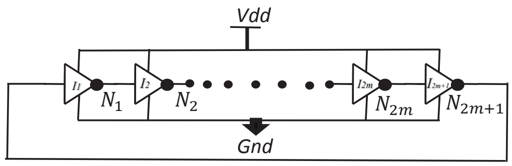

Fig. 1. Typical ring oscillator circuit with $2m$ +1 inverter stages.

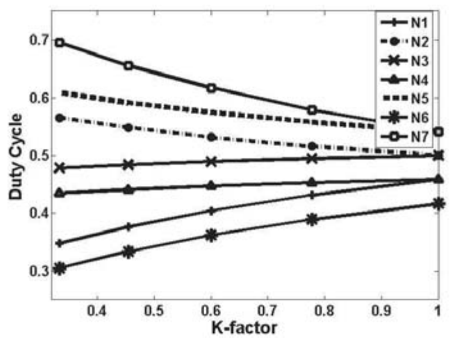

Fig. 2. Duty cycle at the nodes *N1-N7* under different delay ratio *K-factor*.

and fall times, the duty cycle at each inverter output stage is approximately 50%. The duty cycle at each output node can be offset from the 50% value by mismatching the rise and fall delay time of odd and even stages. The capability to produce independent and separate duty cycles at each node provides a method to enhance the entropy of duty cycle values for use in PUF application. A mathematical analysis to justify using a seven-stage ring oscillator is presented below.

A typical ring oscillator circuit with (2*m*+1) stages, where *m* is a positive integer, is shown in Fig. 1. The corresponding high and low time at the output of each node *N1, N2, .. N(2m+1)* can be expressed as

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

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

where *tdf(i)* and *tdr(i)* are, respectively, the fall and rise propagation delay of each inverter stage.

As a case study for a seven stage ring oscillator (*i.e.*, *m=3*, where the rise time between odd and even stages is mismatched by a factor *K-factor=(tdr(i)/tdr(i+1))*, the low and high time at the output and corresponding duty cycle have different values. Theoretical analysis of the duty cycle value using (1) and (2) and a value of *K-factor* ranging from 0.3 to 1, the corresponding duty cycle at each node, *N1* to *N7*, has a different value and changes uniformly with the *K-factor*, as shown in Figure 2. The separation between the duty cycles at each node *N1* to *N7* in Fig. 2 can be increased by using added offset values to fall delay between alternate stages.

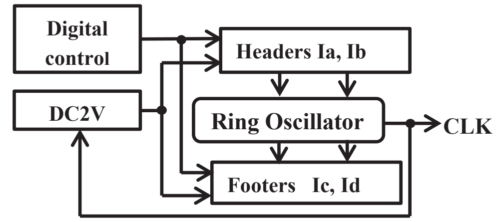

Fig. 3. Block diagram of pulse width modulator.

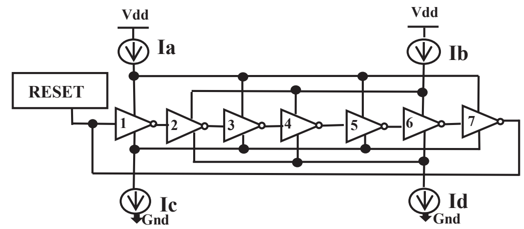

Fig. 4. Seven-stage current controlled ring oscillator.

A digitally controlled pulse width modulator [4] has been proposed to control the ring oscillator rise and fall time at each stage and correspondingly the duty cycle at each stage output. As shown in [4], the digital control provides a versatile and flexible method of generating distinct duty cycle values at the output node of the PWM. A digital current source control feature for the PWM is utilized to demonstrate the proposed controlled and re-configurable PUF circuit primitive.

III. Pulse width modulator

An architectural block diagram of PWM is shown in Fig. 3 where the output of the ring oscillator CLK is fed to the duty cycle to voltage converter (DC2V) block to generate a control signal. DC2V provides an analog control signal for the headers and footers to ensure a stable duty cycle under PVT variations. Digital control provides signals for the header and footer circuits to dynamically change the duty cycle and frequency of the ring oscillator. The details of the digitally controlled PWM and related features are described in detail in [4–6].

A. PWM characteristics

Analytic expressions for the duty cycle and frequency in terms of header and footer currents [4], [5] are summarized here. The circuit schematic of the PWM in terms of header and footer current sources is illustrated in Fig. 4. Referring to Fig. 4, a list of parameters defined for the expressions is as follows $\alpha = IA/IA5$, $\beta = IB/IB5$, $\gamma = IC/IC5$, and $\delta = ID/ID5$ where *IA, IB, IC*, and *ID* are the currents passing through, respectively, *Ia, Ib, Ic,* and *Id*. *IA5, IB5, IC5,* and *ID5* are the currents passing, respectively, through *Ia, Ib, Ic,* and *Id* to provide a 50% duty cycle. The duty cycle and frequency of the PWM are expressed as

$$D = 1/(1 + (\alpha/\beta) * (\gamma/\delta)), \tag{3}$$

978-1-5386-4881-0/18/$31.00 ©2018 IEEE

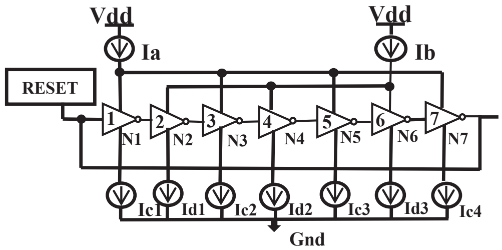

Fig. 5. Modified seven-stage current controlled ring oscillator for PUF application.

$$Fnew = 2 * (1 - D) * F0. \tag{4}$$

where D is the duty cycle of the proposed PWM, *F0* is the frequency of PWM when D is equal to 0.5, and *Fnew* is the new frequency of the PWM. To maintain a constant frequency, the ratio of the header currents (IB/IA) or footer currents (IC/ID) can be determined for each value of duty cycle D as

$$IB/IA = D/(1 - D), \tag{5}$$

$$IC/ID = D/(1 - D). \tag{6}$$

B. PWM circuit as a PUF primitive

The proposed PWM circuit for PUF application is shown in Fig. 5. The footer circuits $Ic1$, $Id1$, $Ic2$, $Id2$, $Ic3$, $Id3$ and $Ic4$ are a set of NMOS transistors connected to each inverter stage to control the sink current of each stage. The footers are controlled with digital inputs to provide the correct current to produce the fall delay offset and accordingly to produce a unique duty cycle at each of the output nodes *N1-N7*. The header circuit provides duty cycle control with digital inputs and PVT compensation capability.

C. PWM Analysis for PUF application

The current controlled variable duty cycle PWM described analytically in (3) is exploited to develop a PUF primitive. Evaluation of the duty cycle at each node *N1* to *N7* of the current controlled PWM is performed using a range of current ratio values for currents *IA* and *IB* from the current sources *Ia* and *Ib*. The corresponding current distribution at odd and even stages is determined for each node *N1* to *N7*, to determine the ratio (α/β) used in (3). The corresponding footer current and ratio (γ/δ) for each node *N1* to *N7* is evaluated and applied in (3). The duty cycle for each node *N1* to *N7* versus header current ratio, *K-factor*=(α/β) is shown in Fig. 6. The current mismatch produces a wide duty cycle distribution for each node over a higher mismatch range of *K-factor*.

IV. Duty Cycle based PUF details

Each PWM based PUF primitive on a chip can be independently configured to produce seven different and independent groups of duty cycle values that can be adaptively changed through digital control inputs. An important requirement of a PUF primitive is to provide distinct values at the output for

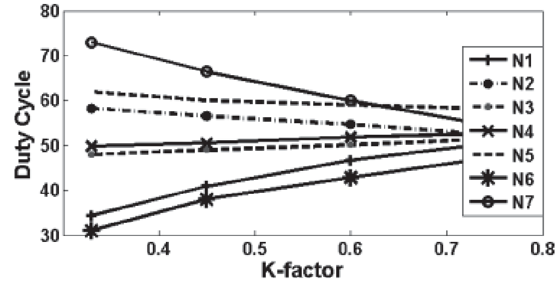

Fig. 6. Duty cycle at nodes *N1-N7* under different current ratio K-factor.

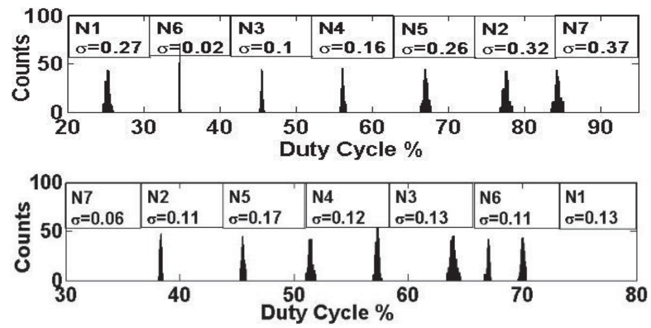

Fig. 7. Duty cycle histogram for $(\alpha/\beta) > 1$ (top), $(\alpha/\beta) < 1$ (bottom).

comparison that are above the error threshold. Additionally, the values should be reliable under environmental changes such as temperature and supply voltage variations. The manufacturing process stable PUF can be randomized with random digital control inputs. The PUF can be adapted to re-configure the PUF duty cycle outputs with digital control. The proposed PUF is evaluated with transistor-level simulations and satisfies the requirements of a feasible PUF primitive.

A. PUF primitive unique outputs

A statistical analysis of the duty cycle is performed with Monte Carlo simulations using 32nm PTM [35] CMOS models. A duty cycle histogram chart of the Monte Carlo simulation of 200 samples of the two different configurations of the header current source ratio for the PUF circuit is shown in Fig. 7. The duty cycle values are distinctly separated with a very low statistical spread which is indicated with low standard deviation value. The proposed PUF circuit provides a wide range of 20%-90% duty cycle outputs based on digital challenge inputs. Accordingly, the proposed PUF can generate a large set of challenge-response pairs for security applications.

B. PVT stable PUF primitive evaluation

The duty cycle comparison based proposed PUF primitive is stable over temperature, voltage, and process variations. The DC2V feedback circuit used in the PWM compensates the header currents over the IC manufacturing process conditions, temperature changes, and supply voltage variations to keep

978-1-5386-4881-0/18/$31.00 ©2018 IEEE

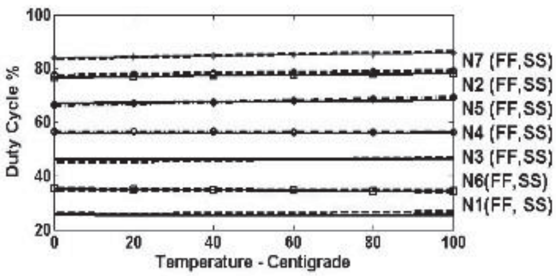

Fig. 8. Temperature versus duty cycle for output nodes *N1-N7*.

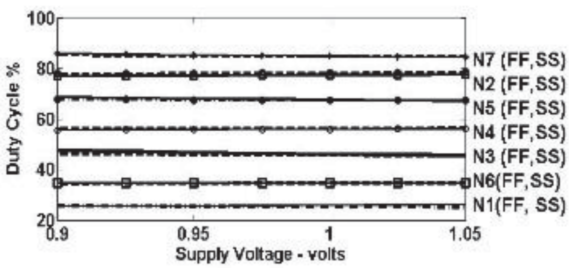

Fig. 9. Supply voltage versus duty cycle for output nodes *N1-N7*.

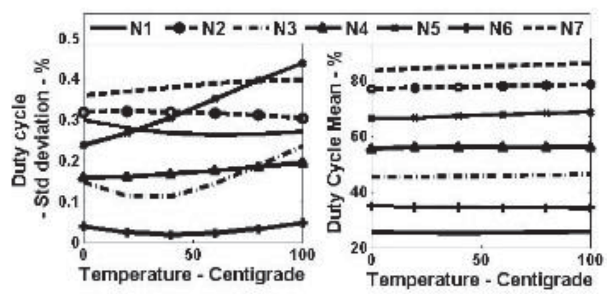

Fig. 10. Standard deviation (left) and mean (right) values of the duty cycle under temperature variations.

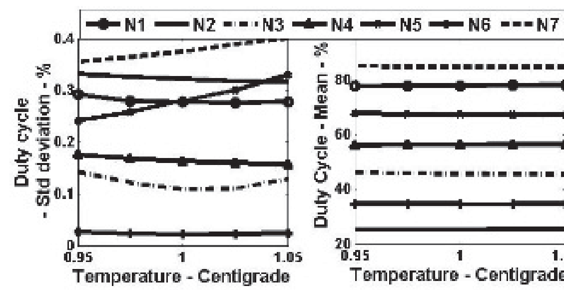

Fig. 11. Standard deviation (left) and mean (right) values of the duty cycle under different supply voltages.

the duty cycle constant to within 1%-2% over the operating ranges. Circuit simulations performed with CMOS 32nm PTM models over SS and FF corners, temperature range of 0°C-100°C, and supply voltage of 1 V are shown in Fig. 8. The duty cycle differences over SS and FF process corners deviate within 1% value for the output nodes *N1* to *N7* and between 1%-2% over temperature range of 0°C-100°C.

Simulation results of duty cycle over the supply voltage range of 0.9V-1.05V, 27°C, for SS and FF process corners, are shown in Fig. 9. The duty cycle at each output node is stable to within 1% between the voltage range of 0.9V to 1.05V over SS and FF process corners.

A typical value of 2% threshold difference for error limits over PVT conditions ensures the validity of unique values for duty cycle comparisons to generate distinct output response bits.

V. Proposed PUF reliability

Monte Carlo circuit simulation of 100 instances of the proposed PUF primitive using 32nm PTM models is performed over the temperature range of 0°C-100°C at 1 V to evaluate the temperature reliability. The variation of standard deviation of the duty cycle (left) and the mean value of the duty cycle (right) over the temperature range of simulation for output nodes *N1-N7* are shown in Fig. 10. The fractional value of the standard deviation and stable duty cycle mean value demonstrates a stable and reliable PUF primitive over temperature. Monte Carlo circuit simulation of 100 instances of the proposed PUF primitive using 32nm PTM models is performed over the supply voltage range of 0.95V-1.05V at 27°C to evaluate the supply voltage reliability. The standard deviation and mean value of the duty cycle is shown in Fig. 11 over the operating voltage range. The standard deviation of the duty cycle is a fractional value for output nodes *N1-N7* with a stable mean value over the supply voltage range.

VI. Conclusion

A variable duty cycle PUF primitive is proposed for security applications. The proposed PUF primitive is demonstrated to be stable over the worst case and best case manufacturing process, supply voltage, and temperate variations. The proposed PUF primitive uses current starved inverters, thus reducing the power requirements. The feedback utilized to maintain a robust duty cycle under PVT variations uses a simple, stable circuit that provides a fast response with an effective compensation over the operating ranges. The proposed PUF primitive is configured and controlled with digital inputs for security adaptation and therefore well suited for programmable applications, portable applications requiring low power and small area.

978-1-5386-4881-0/18/$31.00 ©2018 IEEE

REFERENCES

[1] V. Kursun, S. G. Narendra, V. K. De, and E. G. Friedman, “Low-voltage-swing monolithic dc-dc conversion,” *IEEE Transactions on Circuits and Systems II:Express Briefs*, pp. 241-248, Vol. 51, No. 5 , May 2004.

[2] J. Lee, G. Hatcher, L Vandenberghe, and C. K. Yang, “Evaluation of Fully-Integrated Switching Regulators for CMOS Process Technologies,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* pp. 1017-1027, September 2007.

[3] S. Dhar and D. Maksimovic, “Switching regulator with dynamically adjustable supply voltage for low power VLSI,” *Proceedings of IEEE Annual Conference of the Industrial Electronics Society,* pp. 1874-1879, 2001.

[4] M. J. Azhar and S. Köse, “An Enhanced Pulse Width Modulator with Adaptive Duty Cycle and Frequency Control,” *Proceedings of the IEEE International Symposium on Circuits and Systems,* pp. 958 - 961, May 2014.

[5] I. Vaisband, M. Azhar, E. G. Friedman, and S. Köse, “Digitally Controlled Pulse Width Modulator for On-Chip Power Management,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* Vol. 22, No. 12, pp. 2527 - 2534, December 2014.

[6] S. Köse, I. Vaisband, and E. G. Friedman, “Digitally Controlled Wide Range Pulse Width Modulator for On-Chip Power Supplies,” *Proceedings of the IEEE International Symposium on Circuits and Systems,* pp. 2251 - 2254, May 2013.

[7] I. Vaisband, B. Price, S. Köse, Y. Kolla, E. G. Friedman, and J. Fischer, ”Distributed Power Delivery with 28 nm Ultra-Small LDO Regulator,” *Analog Integrated Circuits and Signal Processing,* Vol. 83, Issue 3, pp. 295 - 309, 2015.

[8] J. Li, Y. Qiu, Y. Sun, B. Huang, M. Xu, D.S. Ha, and F. C. Lee, “ High resolution Duty-cycle schemes for Voltage Regulators,” *Proceedings of Twenty-Second IEEE Applied Power Electronics Conference and Exposition,* pp. 871-876, February 2007.

[9] S. Köse, “Regulator-Gating: Adaptive Management of On-Chip Voltage Regulators,” *Proceedings of the ACM/IEEE Great Lakes Symposium on VLSI,* pp. 105 - 110, May 2014.

[10] S. Köse, S. Tam, S. Pinzon, B. McDermott, and E. G. Friedman, ”Active Filter Based Hybrid On-Chip DC-DC Converters for Point-of-Load Voltage Regulation,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* Vol. 21, No. 4, pp. 680 - 691, April 2013.

[11] S. Köse and E. G. Friedman, “An Area Efficient Fully Monolithic Hybrid Voltage Regulator,” *Proceedings of the IEEE International Symposium on Circuits and Systems,* pp. 2718 - 2721, May/June 2010.

[12] S. Köse and E. G. Friedman, “On-Chip Point-of-Load Voltage Regulator for Distributed Power Supplies,” *Proceedings of the ACM/IEEE Great Lakes Symposium on VLSI,* pp. 377 - 380, May 2010.

[13] I. Vaisband, R. Jakushokas, M. Popovich, A. V. Mezhiba, S. Köse, and E. G. Friedman, On-Chip Power Delivery and Management, Fourth Edition, Springer, 2016.

[14] C. Wang, M. Yan, Y. Cai, Q.Zhou, and J. Yang, “Power Profile Equalizer: A Lightweight Countermeasure against Side-Channel Attack,” *Proceedings of the IEEE Conference on Computer Design,* pp. 305-312, November 2017.

[15] W. Yu and S. Köse, “Exploiting Voltage Regulators to Enhance Various Power Attack Countermeasures,” *IEEE Transactions On Emerging Topics in Computing,* Vol. PP, No. 99, pp. 1-1, 2017.

[16] M. Kar, D. Lie, M. Wolf, V. De, and S. Kukhopadhyay, “Impact of inductive integrated voltage regulator on the power attack vulnerability of encryption engines: A Simulation study,” *Proceedings of the IEEE Custom Integrated Conference,* pp. 1-4, September 2014.

[17] W. Yu and S. Köse, “Charge-Withheld Converter-Reshuffling (CoRe): A Countermeasure Against Power Analysis Attacks,” *IEEE Transactions on Circuits and Systems II: Express Briefs,* Vol. 63, No. 5, pp. 438 - 442, May 2016.

[18] V. Telandro, E. Kussener, A. Malherbe, H. Barthelemy, “On-Chip Voltage Regulator Protecting Against Power Analysis Attacks,”, *IEEE International Midwest Symposium on Circuits and Systems,* pp. 507-511, August 2006.

[19] W. Yu and S. Köse, “A Voltage Regulator-Assisted Lightweight AES Implementation Against DPA Attacks,” *IEEE Transactions on Circuits and Systems I: Regular Papers,* Vol. 63, No. 8, pp. 1152 - 1163, August 2016.

[20] W. Yu and S. Köse, “Security-Adaptive Voltage Conversion as a Lightweight Countermeasure Against LPA Attacks,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* Vol. 25, No. 7, pp. 2183 – 2187, July 2017.

[21] B. Gassend, M. V. Dijk, D. Clarke, and E. Torlak, “Controlled Physical Random Functions and Applications,” *ACM Transactions on Information and System Security,* Vol. 10, No. 4, pp. 4, January 2008.

[22] M. Aman, K. Chua, C. Kee, and B. Sikdar, “Mutual Authentication in IoT Systems using Physical Unclonable Functions,” *IEEE Internet of Things Journal,* Vol. PP, No. 99, pp. 1-1, May 2017.

[23] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijik, and S. Devadas, “A technique to build a secret key in integrated circuits for identification and authentication applications,” *Proceedings of Symposium on VLSI Circuits,* pp. 176-179, June 2004.

[24] B. Gassend, M. V. Dijk, D. Clarke, S. Devadas, ”Silicon Physical Random Functions,” *Proceedings of the ACM Conference on Computer and Communications Security,* pp. 148-160, 2002.

[25] G. E. Suh, S. Devadas, “Physical Unclonable Functions for Device Authentication and Secret Key Generation,” *Proceedings of the Design Automation Conference,* pp. 9-14, June 2007.

[26] C. Herder, D. Yu, F. Koushanfar, and S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial,” *Proceedings of the IEEE,* Vol. 102, No. 8, pp. 1126-1141, August 2014.

[27] C. R Chaudhuri, F. Amsaad and M. Naimat, “Impact of temporal variations on the performance and reliability of configurable ring oscillator PUF,” *Proceedings of the IEEE National Aerospace and Electronics Conference and Ohio Innovations Summit,* pp. 458-463, July 2016.

[28] J. Delvaux and I. Verbauwhede, “Key-recovery Attacks on Various RO PUF Constructions via Helper Data Manipulations,” *Proceedings of the Design, Automation and Test Conference and Exhibition,* pp. 1-6, March 2014.

[29] F. Amsaad, A. Prasad, C. Roychaudhri, M. Naimat, “A Novel Security Technique to Generate Truly Random and Highly Reliable Reconfigurable ROPUF-based Cryptographic Keys,” *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust,* pp. 185-190, May 2016.

[30] G. Komurcu, A. E. Pusane, and G. Dundar, “Dynamic Programming Based Grouping Method for RO-PUFs,” *Proceedings of the 9th Conference on Ph. D. Research in Microelectronics and Electronics,* pp. 329-332, June 2013.

[31] C. Yin, D. En, and G. Ku, “LISA: Maximizing RO PUF’s Secret Extraction,” *Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust,* pp. 100-105, June 2010.

[32] R. Kumar, V. Patil, and S. Kundu, “On Design of Temperature Invariant Physically Unclonable Functions Based on Ring Oscillators,” *Proceedings of the IEEE Computer Society Annual Symposium on VLSI,* pp. 165-170, August 2012.

[33] S. K. Mathew *et al.*, “2.4 Gbps, 7mW All-Digital PVT-Variation Tolerant True Random Number Generator for 45nm CMOS High-Performance Microprocessor,” *IEEE Transactions of Journal of Solid State Circuits,* Vol. 47, No, 11, pp. 2807-2821, November 2012.

[34] J. Augustin and M. L. Lopez-Vallejo, “A Temperature-Independent PUF with a Configurable Duty Cycle of CMOS Ring Oscillators,” *Proceedings of the IEEE Symposium on Circuits and Systems*, pp. 2471-2474, May 2016.

[35] NIMO Group, “Predictive Technology Model (PTM), [Online] http://ptm.asu.edu, Arizona State University.

978-1-5386-4881-0/18/$31.00 ©2018 IEEE