A Hybrid Self-calibration Technique to Mitigate the Effect of Variability in TRNG

Vikram B. Suresh
Dept. of Electrical & Computer Engineering
University of Massachusetts, Amherst, USA
vsuresh@ecs.umass.edu

Wayne P. Burleson
Dept. of Electrical & Computer Engineering
University of Massachusetts, Amherst, USA
burleson@ecs.umass.edu

***Abstract*— In this work, we briefly study the effect of variability in process and operating conditions on the statistics and performance of on-chip True Random Number Generator (TRNG), using the cryptographic measure of bit entropy. Circuits designed in deep submicron technologies are susceptible to variation in process. The variability may affect the circuit performance, power and reliability. Numerous pre-silicon design methodologies and post-silicon circuit tuning mechanisms have been proposed in literature. We propose a hybrid self-detection and calibration technique based on algorithmic post processing and circuit tuning to mitigate the effects of variability. Results show that variation in fabrication process and varying on-chip temperature affect the reliability of these circuits. On employing the proposed self calibration technique in 45nm technology, an improvement of close to 4X in the bit entropy is seen across a range of 10% intra-die variation. The proposed technique also mitigates the effect of variation in operating temperature. The simple control logic has an estimated area of 128 um^2 and results in a negligible energy overhead of 0.82 fJ/bit.**

I. INTRODUCTION

Variation in the fabrication process is emerging as a major challenge in IC design and manufacturing [1]. The effect of process variation is no longer limited to the yield and reliability of the designs. It may also manifest in the form of degraded performance and higher power dissipation. Apart from process, designs are also affected by the variation in operating conditions. With shrinking feature sizes and reducing supply voltage, designs are more sensitive to variation in operating temperature and noise on the power supply. These issues have necessitated rigorous analysis of circuit timing and power at the design phase. Statistical timing and power analysis are performed across multiple process corners and operating conditions. But, there is a limit to the guard band that can be provided against variability, considering the need for high performance and low power systems. Hence, there has been an advent of on-chip compensation circuits in the last decade.

Analog circuits are most sensitive to Process, Voltage and Temperature (PVT) conditions. A number of circuit calibration techniques have been proposed in literature to compensate for variability. In [2], X. Li *et al.* have proposed an adaptive post-silicon tuning method for analog circuits. A digital calibration technique for analog circuits, using programmable capacitor stack is described in [3]. One of the most prominent tuning techniques for digital circuits has been Adaptive Body Biasing (ABB). ABB is employed to vary body bias to control the threshold voltage of transistors and hence compensate for variation due to fabrication process [4] [5]. In [6], S. Bijansky *et al.* have proposed the use of variable supply voltages to improve parametric yield of designs. Variable delay buffers have also been extensively used to tune the delay on paths, primarily the clock paths. These provide a flexible solution to configure the buffer strengths based on the degree of process variation [7]. The variable delay tuning techniques may be implemented both in the form of tuning at the testing phase or online automatic/adaptive tuning [8]. Apart from the generic data paths and clock paths, special on-chip circuitry like sensors and detectors are also susceptible to variation in manufacturing process and operating conditions. Along with performance, the efficiency of these circuits is also affected by variability. B. Dutta *et al.* [9] have proposed calibration of thermal sensors using process monitors to increase the robustness of the sensors in the presence of variation. With the increasing use of hardware cryptographic primitives in various applications, on-chip TRNGs, designed in advance technology nodes are also affected by variation in process and operating conditions. These variabilities affect the statistics of random number generators, in turn degrading the bit rate and energy efficiency.

In this work, we propose a hybrid method, which includes traditional algorithmic techniques and modern circuit calibration to mitigate the effect of PVT variation. The rest of this paper contains the background and motivation in section II, the effect of variability in section III, the proposed hybrid technique in section IV, followed by results and conclusions in sections V and VI respectively.

II. BACKGROUND AND MOTIVATION

True random number generators (TRNG) are circuits that sample a random physical phenomenon like, thermal noise and digitize it for use for cryptographic applications. One of the most commonly used circuits for random number generation is ring oscillator (RO) which uses jitter as the source of randomness [10]. A basic RO based TRNG uses two or more ring oscillators and the outputs are XORed. The output signal of the XOR when sampled in the transition zone generates random bits due to random jitter in the two oscillator rings [11]. Although RO based TRNG are easier to implement, they have limited data rate and consume more energy per bit. Hence, a new class of TRNG circuits, based on metastable circuits, is emerging for high performance and low energy cryptographic applications. These circuits may use power up state of on-chip SRAM [12] or a bi-stable element using cross coupled inverters

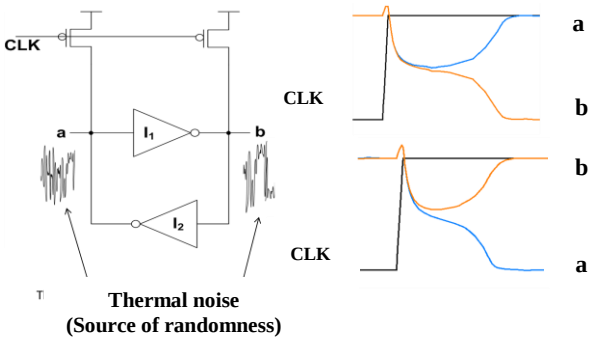

Figure 1: Metastability based TRNG

In this work we demonstrate the proposed self-calibration technique on a TRNG circuit using a pair of cross coupled inverters, fig [1], along with pre-charge to generate random bits [13]. The inputs of the two inverters are pre-charged to VDD and then allowed to resolve state. Based on the thermal noise at the input of the two inverters, the output resolves either to bit '1' or bit '0'. One of the basic measures of randomness of a TRNG is the bit entropy *H(x)*,

$$H(x) = -p(0)\log_2 p(0) - p(1)\log_2 p(1) \qquad (1)$$

where p(0) and p(1) are the probability of bits '0' and '1' respectively. An ideal TRNG should generate equal number of zeros and ones, thereby providing bit entropy of '1'. This is possible only when all the transistors of the two inverters are correspondingly matched. But, intra-die variations lead to mismatch in the devices. This may bias the circuit to resolve its state to a '0' or a '1' with higher probability. Then the behavior of the circuit is governed not only by the random thermal noise, but also by the degree of intra-die variation. This affects the statistics of the circuit and decreases the bit entropy. The two main approaches to mitigate the effect of process variation are through algorithmic techniques or circuit calibration.

The most basic algorithmic approach is the XOR function. When the output of two or more TRNG is XORed, the entropy of the resulting bit stream is greater than the individual entropies. Another commonly used technique is von Neumann corrector [11]. A von Neumann corrector reads consecutive pairs of bits from the TRNG and outputs a '0' for a '10' pair, a '1' for a '01' pair and no output otherwise. Although the von Neumann technique mitigates the effect of variability, the bit rate is halved. In [13], a two stage circuit calibration technique has been proposed using parallel NMOS and PMOS stacks that are configured to reduce the device mismatch. A variable delay line on the pre-charge clock is used to provide a finer control to calibrate the circuit. V. Suresh *et al.* [14], have performed an analysis of the trade-off between these techniques with respect to mitigation of effect of process variation and the energy overhead for the same. It is seen that circuit calibration provides efficient correction consuming minimal energy per bit.

Circuit calibration performed during chip testing adds an overhead to the testing time. This affects the cost and productivity of the chip. Further, calibration performed at the testing phase accounts only for the initial process variation. It does not mitigate the effects of operating conditions and the possible degradation of the circuit due to wear out effects. Hence there is a need for adaptive self-calibration. Srinvasan *et al.* have proposed a self-calibration mechanism using circuit tuning methods [15]. The technique uses an adaptive two stage calibration to operate the TRNG close to a state equivalent to zero device mis-match. But, such an approach needs to tune the circuit every cycle adding to the energy overhead. Complex control logic is necessary to perform efficient calibration, adding to area and power overhead. A cycle-to-cycle circuit tuning may also introduce correlation between the bits generated. These factors serve as motivation to come up with an efficient, robust and cost effective self-calibration technique with minimal area and energy overhead. In this paper, we propose a hybrid self-calibration technique that utilizes the flexibility of circuit calibration to provide a one-time coarse level tuning followed by the low overhead algorithmic approach for continuous calibration.

III. Effect of Variability

A. *Variation in process*

Metastability based TRNG use circuits that extract entropy from random physical sources. Hence these circuits are highly sensitive to process variation. Even a small mismatch in the device parameters can weaken the statistics of the random number generator. The randomness of the bits generated, measured in terms of bit entropy, decreases with increasing device mismatch. The plot, fig [2] indicates that the circuit is highly vulnerable to process variability. With increase in intra-die variation and hence the device mismatch, the bit entropy of the output decreases. The XOR function provides effective compensation only for small variations. The von Neumann correction technique protects the design from the effect of variability by maintaining the entropy very close to the ideal value of '1'. But, the output bit rate drastically falls with increasing device mismatch.

B. *Variation in operating temperature*

TRNG circuits are also affected by the variation in operating temperature. The performance of transistors degrades with increase in temperature. But, it is observed that the degradation is also a function of the transistor parameter, like the channel length, fig [3]. Devices with different channel lengths are observed to have different gradients in the decrease of ON current. The robustness of circuits like the TRNG depends on the relative difference in transistor performance, rather than the absolute variation. Hence, varying temperature has greater impact in the case of larger intra-die variation. Calibration during chip testing cannot account for variability in operating conditions.

C. *Variation in supply voltage*

Although variation in operating voltage affects the performance of circuits, it is observed to have a common mode effect on all the transistors of the TRNG. Hence, for a given process corner, the behavior of the TRNG is observed to remain consistent even in the presence of voltage variation. The statistics of the TRNG is not affected by power supply variability. Thus, in this work we emphasize on the effect of process variation and operating temperature on the TRNG.

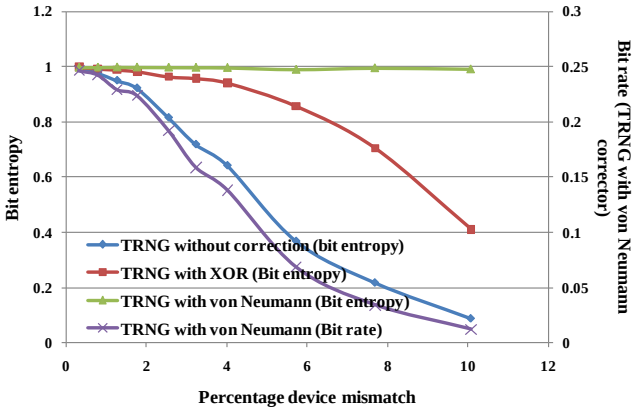

Figure 2: Effect of process variation on bit entropy

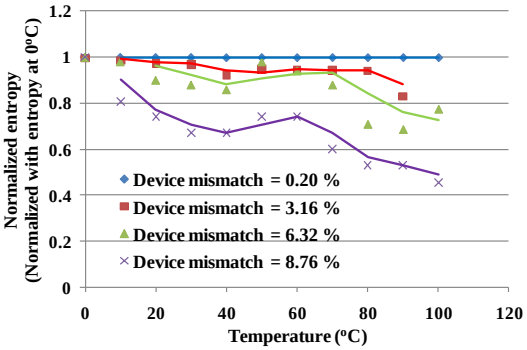

Figure 3: Effect of temperature variation on bit entropy

IV. PROPOSED HYBRID SELF-CALIBRATION TECHNIQUE

Algorithmic post-processing techniques are energy efficient, but not effective for large device mismatches. On the other hand, circuit calibration provides a good trade-off between variability mitigation and energy overhead. We propose a hybrid self-calibration methodology to leverage both these techniques. The hybrid method uses self detection and calibration to provide a one-time coarse grain tuning to nearly match the devices. This is followed by an algorithmic post-processing stage in the form of XOR function or von Neumann corrector to compensate for the remaining mismatch.

Since the cross coupled inverters in the design are pre-charged and then allowed to resolve state, even a small mismatch in the channel length of the two NMOS pull-down transistors can bias the circuit to generate more '0' or '1'. The PMOS pull-up transistors do not play such a significant role. Hence, calibration is provided in the form of parallel NMOS transistors that can be turned ON using configuration bits, fig 4. The transistors along the weaker of the two pull-down devices are configured to provide additional parallel sink paths and hence compensate for the intra-die variation. Control logic monitors the output of the TRNG. Based on whether the output bit is a '1' or a '0', the inverters I1 or I2 is tuned respectively. The self-calibration stops when output bit flips twice. From this stage, the XOR function or the von Neumann corrector further compensate for the fine mismatch and operate the circuit in a region very close to ideal operation as shown in fig 6.

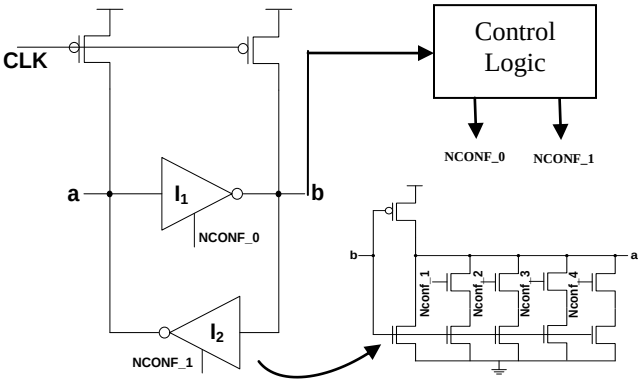

Figure 4: Self-detection and calibration circuit for coarse tuning

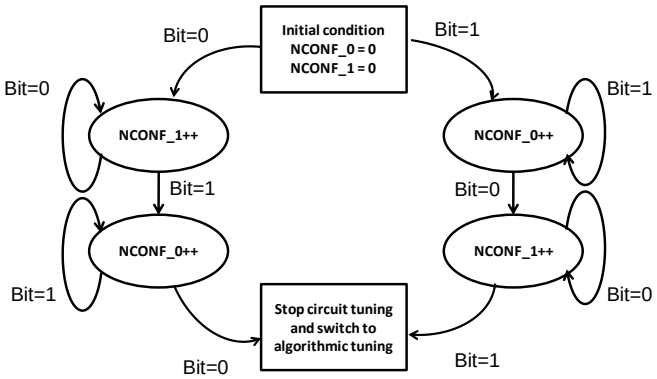

Figure 5: State machine of the control logic

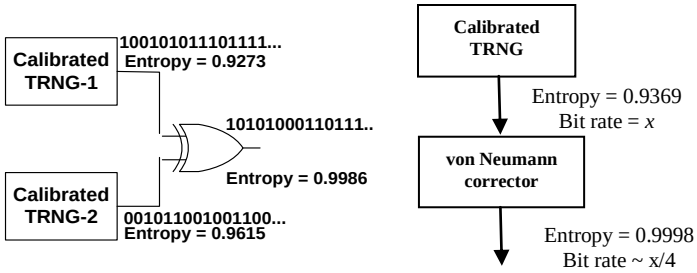

Figure 6: Algorithmic post-processing for fine tuning

V. EXPERIMENTAL SETUP AND RESULTS

The proposed self-calibration technique was implemented using 45nm NCSU PDK. The TRNG circuit along with the configurable transistors was simulated in HSPICE on a Perl based platform. The control logic was described in verilog and synthesized using Synopsys Design Compiler. The results indicate that the coarse grain self-calibration compensates for the variability to a large extent by enhancing the bit entropy to values greater than 0.95. The stand alone circuit calibration is observed to be more effective for large device mismatches due to the coarse level of tuning.

The hybrid method of algorithmic post-processing applied in conjunction with self-calibration, makes the TRNG circuit more robust against process variation. The design with two TRNG circuits, with initial self-calibration followed by an XOR of their outputs almost nullifies device mismatch. The values of bit entropy remain consistently around the ideal value of '1' for a wide range of intra-die variation. A similar

approach with a self calibrated TRNG feeding a von Neumann corrector also completely mitigates the effect of variability on the performance of the TRNG. A plot of the bit rate of the TRNG with the stand alone von Neumann correction and the hybrid self-calibration shows a steady bit rate even for device mismatches as large as 10%. This facilitates the design of high speed cryptographic systems using hardware primitives designed in the latest technology node.

Apart from process variation, the hybrid calibration technique also improves the reliability of the TRNG circuit in varying operating conditions. An analysis of the proposed technique across varying temperature for different degree of device mismatches shows are as shown in fig 8. The results clearly show that the behavior of the TRNG is maintained even in the presence of device mismatch and varying thermal profiles.

The self-calibration technique does add an overhead both in terms of area and energy. The area of the control logic is 128um^2, which is negligibly small compared to the modern processors and cryptographic cores. Since the self calibration logic operates only during the initial cycles, till the output bit flips for the first time, it only contributes to the overhead power in the form of static power in the long run. The static power of the control logic was estimated to be 819.08nW. This translates into 0.82 fJ/bit for a TRNG operating at 1Gbps with a worst case overall energy per bit of 0.5pJ/bit.

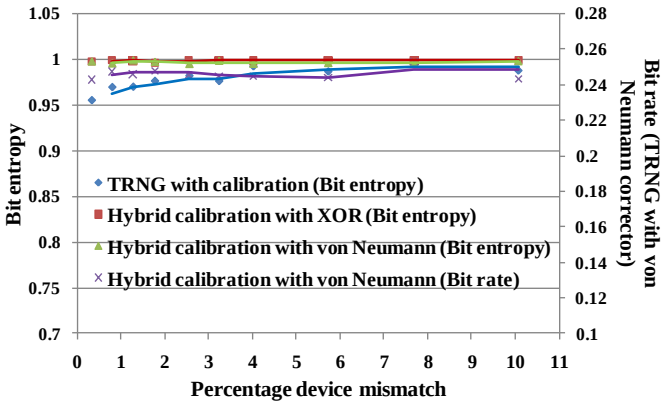

Figure 7: Variation of bit entropy with hybrid self-calibration (von Neumann)

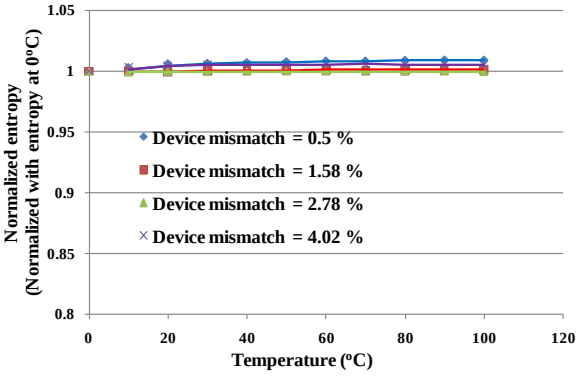

Figure 8: Self-calibration enhancing reliability of TRNG across temperature ranges

VI. CONCLUSION

Variability in manufacturing process and operating conditions hamper the performance and efficiency of circuits in deep submicron technologies. A hybrid self-calibration technique has been proposed to mitigate the effect of process variation and operating temperature on cryptographic primitives like TRNG. The technique makes use of existing algorithmic post-processing methods along with self-detection and calibration circuit. Results show a significant improvement in the reliability of the TRNG against variability. Improvement of upto 4X in both the bit entropy and the bit rate is observed across a device mismatch as large as 10%. The solution employs a simple control logic, resulting minimal overhead in power and design area. The hybrid self-calibration technique provides a reliable, cost effective and low overhead solution to mitigate the variability. The proposed solution may is not restricted to cryptographic hardware and can be extended to generic circuit design issues as well.

REFERENCES

[1] "The International Technology Roadmap for Semiconductors."

[2] Xin Li, B. Taylor, YuTsun Chien, and L. Pileggi, "Adaptive post-silicon tuning for analog circuits: concept, analysis and optimization," *Computer-Aided Design, 2007. ICCAD 2007. IEEE/ACM International Conference on*, 2007, pp. 450-457.

[3] Wei Yao, Yiyu Shi, Lei He, and S. Pamarti, "Joint design-time and post-silicon optimization for digitally tuned analog circuits," *ICCAD 2009*.

[4] S. Kulkarni, D. Sylvester, and D. Blaauw, "Design-Time Optimization of Post-Silicon Tuned Circuits Using Adaptive Body Bias," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, vol. 27, 2008, pp. 481-494.

[5] S. Kulkarni, D. Sylvester, and D. Blaauw, "A Statistical Framework for Post-Silicon Tuning through Body Bias Clustering," *Computer-Aided Design, 2006. ICCAD '06. IEEE/ACM International Conference on*, 2006, pp. 39-46.

[6] S. Bijansky, Sae Kyu Lee, and A. Aziz, "TuneLogic: Post-silicon tuning of dual-Vdd designs," *Quality of Electronic Design, 2009. ISQED 2009. Quality Electronic Design*, 2009, pp. 394-400.

[7] D. Tadesse, J. Grodstein, and R. Bahar, "AutoRex: An automated post-silicon clock tuning tool," *ITC 2009.*

[8] K. Nagaraj and S. Kundu, "An Automatic Post Silicon Clock Tuning System for Improving System Performance based on Tester Measurements," *Test Conference, 2008. ITC 2008. IEEE International*, 2008, pp. 1-8.

[9] B. Datta and W. Burleson, "Calibration of on-chip thermal sensors using process monitoring circuits," *Quality Electronic Design (ISQED), 2010 11th International Symposium on*, 2010, pp. 461-467.

[10] V. Fischer, F. Bernard, N. Bochard, and M. Varchola, "Enhancing security of ring oscillator-based trng implemented in FPGA,", in *FPL 2008*.

[11] B. Sunar, W. Martin, and D. Stinson, "A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks," *Computers, IEEE Transactions on*, vol. 56, 2007,

[12] D. Holcomb, W. Burleson, and K. Fu, "Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers," *Computers, IEEE Transactions on*, vol. 58, 2009, pp. 1198-1210.

[13] S. Srinivasan, S. Mathew, V. Erraguntla, and R. Krishnamurthy, "A 4Gbps 0.57pJ/bit Process-Voltage-Temperature Variation Tolerant All-Digital True Random Number Generator in 45nm CMOS," *VLSI Design, 2009 22nd International Conference on*, 2009, pp. 301-306.

[14] V. Suresh and W. Burleson, "Entropy extraction in metastability-based TRNG," *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*, 2010, pp. 135-140.

[15] S. Srinivasan, *et al.*, "2.4GHz 7mW all-digital PVT-variation tolerant True Random Number Generator in 45nm CMOS," *VLSI Circuits (VLSIC), 2010 IEEE Symposium on*, 2010, pp. 203-204.