Robust Metastability-based TRNG Design in Nanometer CMOS with Sub-Vdd Pre-charge and Hybrid Self-calibration

Vikram B. Suresh and Wayne P. Burleson
Dept. of Electrical and Computer Engineering
University of Massachusetts, Amherst
{vsuresh, burlseon}@ecs.umass.edu

Abstract

In this work, we study the impact of sub-vdd pre-charge operation of metastability-based True Random Number Generator (TRNG) and propose a hybrid self-calibration to improve the statistics of the TRNG in the presence increasing intra-die variation. Circuits designed in deep submicron technologies are susceptible to process variation. The variability may affect the circuit performance, power and reliability. Numerous pre-silicon design methodologies and post-silicon circuit tuning mechanisms have been studied in literature. We propose a sub-vdd pre-charge technique to improve the tolerance of the TRNG to device mismatch. This is followed by a hybrid self-detection and calibration technique based on algorithmic post processing and circuit tuning to mitigate the effects of variability. The cryptographic metric of 'bit entropy' is used to validate the proposed techniques. The TRNG circuit and the proposed techniques are implemented using 45nm PDK. Results show that variation in fabrication process affect the reliability of TRNG circuits. Pre-charging the TRNG to 0.7V for a typical supply voltage of 1.1V reduces the impact of device mismatch on the circuit by 2X for device mismatch as large as 4-5%. The hybrid self-calibration further improves the bit entropy by ~120% across a range of 5% intra-die variation. The simple control logic has an estimated area of 128 um^2 and results in a negligible energy overhead of 0.82 fJ/bit.

Keywords

TRNG, Intra-die variation, Entropy, Hybrid Self-calibration

1. Introduction

Variation in 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 variation due to 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 extensive research regarding on-chip compensation circuits in the last decade.

A number of circuit calibration techniques have been proposed in literature to compensate for variability. X. Li *et al.* have proposed an adaptive post-silicon tuning method for analog circuits in [2]. 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]. S. Bijansky *et al.* have proposed the use of variable supply voltages to improve parametric yield of designs in [6]. 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 sense amplifiers, sensors and detectors are also susceptible to variation in manufacturing process and operating conditions. Along with performance, the reliability of these circuits is also affected by variability. Sense amplifier performance and yield degrade with increasing device mismatch, thereby affecting the performance of on-chip cache [9]. B. Dutta *et al.*[10] 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. The variabilities in process and operating conditions affect the statistics of random number generators, in turn degrading the bit rate and energy efficiency.

In this work we propose a robust metastability based TRNG with sub-Vdd operation and hybrid self-calibration to alleviate the effect of on-chip variation. The rest of this paper is organized as follows: Background on TRNG in section 2, sub-vdd pre-charge operation in section 3, hybrid self-calibration in section 4, experimental setup and results in section 5 and finally conclusion and scope for future work in section 6.

2. True Random Number Generator

A True Random Number Generator is a circuit that samples and digitizes a random physical phenomenon. The source of randomness could be on-chip thermal/shot noise, stray electromagnetic field or random quantum phenomenon. On-chip TRNG are being extensively used for generating secret

keys, nonce and seed cryptographic primitives like Pseudo-Random Number Generators (PRNG). The reliability of TRNG is of paramount importance to the security of a cryptographic system. Traditionally, ring oscillator (RO) based TRNG have been used owing to the simplicity in their implementation both in custom chips as well as FPGA [11, 12]. Analog circuits for TRNG have been proposed using A/D converters and oscillators [14]. The power up state of SRAM cells [15], collision between DRAM access and refresh [16], resolution time of metastable elements (using cross-coupled inverters) have been demonstrated to generate random bits [17].

Ring Oscillator based TRNG circuits require the output of multiple rings to be XORed to achieve good statistics. This results in a large amount of dynamic power. Further, RO based TRNG circuits are proved to be susceptible to active attacks like frequency injection attack [13]. TRNG circuits using on-chip memory (SRAM/DRAM) may not be flexible to generate random bits frequently. Thus, TRNG circuits based on metastable elements are gaining prominence. A cross-coupled inverter based metastable element can be used as TRNG fig. 1. The circuit consists of a pair of cross coupled inverters whose output nodes 'a' and 'b' are pre-charged to Vdd during the negative half of the clock cycle. When the pre-charge is released during the positive half cycle, the circuit initially moves towards a metastable state. However, depending on the differential thermal noise at the diffusion of the two gates, the output nodes 'a' and 'b' are resolved to a stable state of 0 (bit = 0) or Vdd (bit = 1), fig. 2. The TRNG has negligibly small area and can be operated at extremely high frequencies. The small circuit size also leads to lower power consumption or energy/bit. Variation in the operating temperature and noise on the power supply act as a common mode effect on the TRNG. Although the metastability based TRNG has visible advantages over contemporary TRNG circuits, local variation due to Random Dopant Fluctuation (RDF) or channel length variation (L_{eff}) may introduce mismatch in the devices of the two inverters. This biases the TRNG to generate more '0' or '1', degrading the statistics of the bit stream generated.

The bias in the TRNG can be corrected by compensating for the mismatch using post-Si tuning or through algorithmic post-processing. XOR function [11], von Neumann correction [11], hash [15] and ciphers are some of the commonly used algorithmic post-processing techniques. Srinivasan *et.al* proposed a post-Si circuit calibration technique for metastability based TRNG in [18]. The technique involves a coarse grain calibration using additional NMOS and PMOS transistors configured in parallel to the cross coupled inverters to compensate for the mismatch. They also propose a fine grained calibration technique to control the pre-charge clock to delay the release of pre-charge on one of the nodes. An adaptive technique to perform automatic calibration is presented in [19]. Suresh *et.al* [20], present a comparative study of the effectiveness of circuit calibration and algorithmic techniques in terms of improvement in the randomness of the bits generated and the energy overhead.

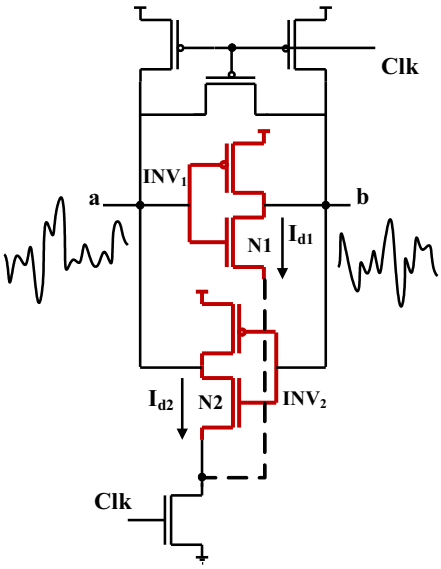

Figure 1: Metastability-based TRNG

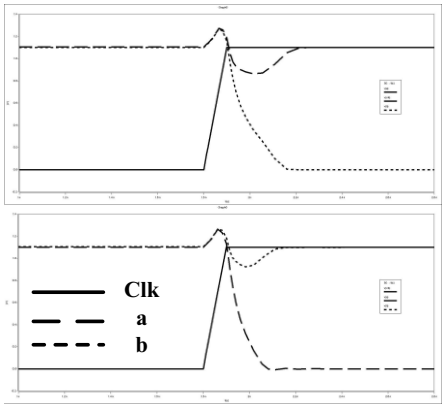

Figure 2: Operation of metastability-based TRNG

Algorithmic post-processing techniques like XOR function and von Neumann corrector are found to be effective only for small ranges of device mismatch. The circuit calibration provides a better trade-off between the degree of correction and the energy overhead. However, calibration at the testing phase involves multiple iterations leading to additional test cost. Online calibration techniques need additional control logic and increase the correlation of the bits generated.

In this work, we analyze the operation of the TRNG in sub-Vdd regime to make the TRNG inherently more robust to intra-die variation. We then propose a hybrid self-calibration technique that involves one-time circuit calibration to compensate for large static variations followed by algorithmic post-processing to correct finer mismatch and mitigate the effect of dynamic variations like temperature.

3. Metastability based TRNG with sub-Vdd pre-charge

This section provides a detailed analysis of the impact of pre-charge voltage on the bias of the TRNG. In fig.1, if all devices of the inverters, INV_1 and INV_2 are ideally matched, the stable state to which the output resolves after entering the metastable state depends solely on the random thermal noise at the two nodes, fig. 2. In such a scenario, the larger

of the two currents I_{d1} and I_{d2}, drive the corresponding node to a '0' and the opposite node to '1' and the TRNG generates bits of both polarity with equal probability. If the mismatch leads to $I_{d1} > I_{d2}$ for *V(a) = V(b)*, the TRNG circuit is biased to generate bit 0 than bit 1 (at node b). This reduces the randomness of the bits generated and affects the security of the system using the TRNG.

Traditional correction techniques for a biased TRNG include post-Si tuning or algorithmic post-processing. Post-Si tuning uses additional transistors to compensate for the mismatch of the devices. The algorithmic post-processing techniques do not modify the TRNG circuit; but, they extract randomness out of the biased bits generated by the raw TRNG circuit.

A closer study of the TRNG circuit shows that when the pre-charge is released, both the pull down NMOS transistors of the inverters enter the saturation mode. The basic saturation current equation (neglecting the short channel effects) is given by [21],

$$I_{dsat} = \frac{\mu_0 c_{ox} W}{2L} \left(V_{gs} - V_t\right)^2 \quad (1)$$

Equating the constants to a value *"β"* and adding a random variable for thermal noise at the gate,

$$I_{dsat} = \frac{\beta W}{L} \left(V_{gs} + V_{noise} - V_t\right)^2 \quad (2)$$

For the metastability based TRNG circuit, the drain current of the two pull down NMOS devices, once the pre-charge is released, is given by,

$$I_{dsat1} = \frac{\beta W_1}{L_1} \left(V_{gs} + V_{noise1} - V_{t1}\right)^2 \quad (3)$$

$$I_{dsat2} = \frac{\beta W_2}{L_2} \left(V_{gs} + V_{noise2} - V_{t2}\right)^2 \quad (4)$$

Under ideal conditions, when the NMOS devices are perfectly matched, $I_{dsat1} = I_{dsat2}$ for $V_{noise1} = V_{noise2}$. In other words, the state of the TRNG is resolved based only on the differential thermal noise $\Delta_{noise} = V_{noise1} - V_{noise2}$. If the NMOS devices are mismatched due to random local variation, the bias in the TRNG can be represented by the difference in the saturation currents at zero differential thermal noise. Thus, for a biased TRNG,

$$I_{dsat1} - I_{dsat2} > 0, for\ V_{noise1} = V_{noise2} \quad (5)$$

Larger the mismatch, larger will be the difference in the currents and hence the bias in the TRNG.

Case 1: Mismatch in NMOS width/length:

In context of a mismatch in the device feature size (width or length) with constant V_t, the difference in the NMOS currents is given by,

$$I_{dsat1} - I_{dsat2} = \left(\frac{\beta W_1}{L_1} - \frac{\beta W_2}{L_2}\right) \left(V_{gs} + V_{noise} - V_t\right)^2 \quad (6)$$

Equation *(6)* indicates that the mismatch in the NMOS devices is magnified by the factor $\left(V_{gs} + V_{noise} - V_t\right)^2$. Since, V_{noise} is a random variable and cannot be controlled, for a given device type (Typical/High/Low V_t), the effect of device mismatch can be reduced by lowering the V_{gs}. Hence, a lower pre-charge voltage can alleviate the effect of process variation.

Considering the short channel effect of variation in length on the threshold voltage [21],

$$\Delta V_{th}(SCE, DIBL) = -\theta_{th}(L_{eff})[2\,(V_{bi} - \phi_s) + V_{ds}] \quad (7)$$

where, ΔV_{th} is the change in threshold due to Short Channel Effect (SCE) or Drain Induced Barrier Lowering (DIBL); $\theta_{th}(L_{eff})$ is the short channel effect coefficient; V_{bi} is the built-in junction voltage; and V_{ds} is the drain-source voltage. In the cross-coupled inverter, the gate voltage of one inverter is the drain-source voltage of the pull down device of the other inverter. Hence, a lower pre-charge voltage reduces the impact of SCE/DIBL effects on the transistors. This further minimizes the degree of mismatch between the NMOS devices.

Case 2: Mismatch in NMOS threshold voltages:

For a mismatch in the threshold voltages of the pull down transistors of the TRNG, the bias, represented as the difference in the saturation currents is,

$$I_{dsat1} - I_{dsat2} = \left(\frac{\beta \mathrm{W}}{\mathrm{L}}\right) \left[\left(V_{gs} + V_{noise} - V_{t1}\right)^2 - \left(V_{gs} + V_{noise} - V_{t2}\right)^2\right] \quad (8)$$

$$I_{dsat1} - I_{dsat2} = \left(\frac{\beta \mathrm{W}}{\mathrm{L}}\right) \left[\left(2V_{gs} + 2\,V_{noise} - V_{t1} - V_{t2}\right) \times \left(V_{t2} - V_{t1}\right)\right] \quad (9)$$

Equation *(9)* also shows that a reduced V_{gs} due to sub-Vdd pre-charge can decrease the impact of mismatch on the bias of the TRNG.

A similar analysis performed with variation in both width/length and threshold voltages also indicate that a lower pre-charge alleviates the impact of intra-die variation on the statistics of the TRNG. Thus, sub-Vdd pre-charge makes the TRNG more robust to variability in fabrication process. Since only the pre-charge voltage is reduced and not the supply voltage, the technique does not impact the performance of the TRNG. However it should be noted that the proposed technique only reduces the pre-charge voltage to less than Vdd, but does not operate the TRNG circuit in sub-threshold mode.

To further validate the hypothesis that lower pre-charge voltage minimizes the effect of intra-die variation, the cross coupled inverter circuit was simulated with varying amount of device mismatch. In fig. 3, if the pull down NMOS N_1 is faster than N_2, then $I_1 > I_2$ for *V(a) = V(b)*. But, for a large enough $\Delta V = V(b) - V(a)$, $I_1 = I_2$. This is the differential voltage required to negate the mismatch and equalize the pull down currents. From the transistor current equation *(6)*, it is

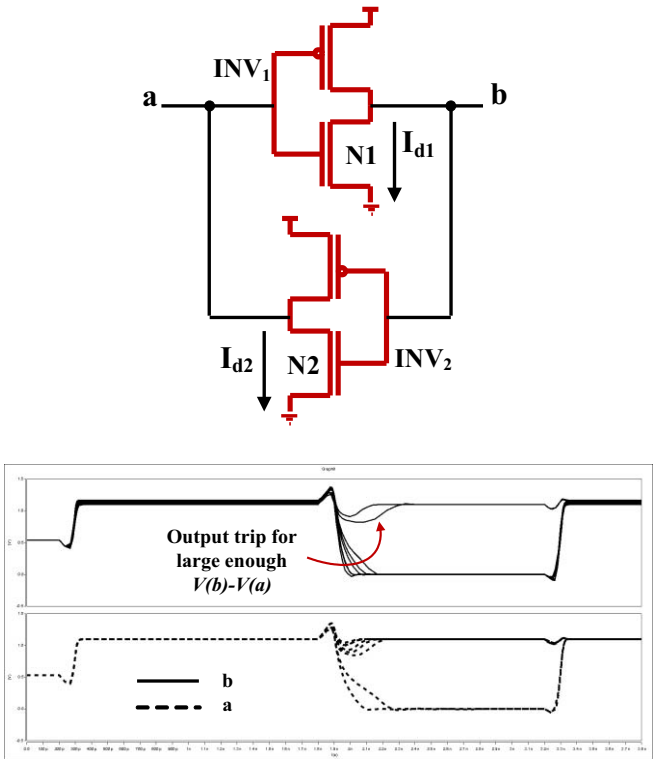

Figure 3: Effect of increasing differential voltage on biased TRNG

evident that a larger mismatch will require a greater differential voltage to overcome the difference in the currents. A plot of the differential voltage required to equalize the pull down currents of cross coupled inverters for varying degree of device mismatch is as shown in fig. 4. The plot shows that for a pre-charge voltage of 1.1V (Vdd) and a device mismatch of 5%, the differential voltage required to nullify the variation is 53mV. For the same mismatch and a pre-charge voltage of 0.75V, the differential voltage required is 34mV. This is because the lower pre-charge voltage results in a lower V_{gs} for the pull down transistors and from equation *(6)*, this minimizes the difference in drain currents. Hence, a smaller differential voltage is sufficient to overcome the mismatch.

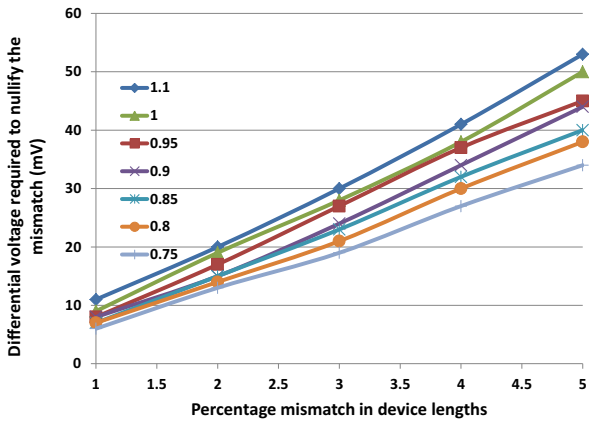

Figure 4: Analysis of differential voltage to compensate mismatch

4. Hybrid self-calibration technique

Reducing the pre-charge voltage can only reduce the impact of variation on the TRNG bias. However, the randomness of the output bits may still not qualify for cryptographic applications and hence need additional calibration or post-processing. The randomness of the output of a TRNG is measured using a number of statistical metrics like bit entropy, byte entropy, autocorrelation factor, bit frequency and so on. Statistical test suits [22] are used to qualify random number generators. In this work we use bit entropy as the metric for randomness. Although bit entropy is a necessary condition to satisfy the randomness test, it is not a sufficient condition for the TRNG to be used for cryptographic applications. However, bit entropy provides a simple technique to study the effect of variation on the statistics of the TRNG. The bit entropy is given by,

$$H = -[\log_2 P(0) + \log_2 P(1)] \qquad (10)$$
$$where, P(0) = Probability\ of\ bit\ 0$$
$$P(1) = Probability\ of\ bit\ 1$$

An ideal TRNG has *P(0) = P(1) = 0.5* and hence an entropy *H = 1*. But, with increase in bias, the probabilities are unequal leading to entropy less than 1.

Algorithmic post-processing is not effective for large device mismatches. While the entropy extracted from the biased bits reduces with increasing mismatch when XOR function is used, the output bit rate of the TRNG decreases with von Neumann correction. Circuit calibration, although effective, incurs additional testing cost if done during the post-Si testing. Adaptive on-chip calibration requires additional control logic to continuously monitor the output of the TRNG and change the configuration bits. The frequency of such a calibration also determines the dynamic power overhead and the secondary effects in the form of increased bit correlation. So, we propose a hybrid self-calibration technique using a combination of one-time adaptive circuit calibration and algorithmic post-processing. The circuit is adaptively calibrated on power-up to compensate the coarse device mismatch. This is followed by continuous algorithmic post-processing to correct the output bits for fine mismatch and account for dynamic variation in operating temperature.

An analysis of the effectiveness of various compensation techniques, fig. 5, show that algorithmic techniques are efficient for upto 2% device mismatch. A one-time adaptive circuit calibration is performed to remove the coarse mismatch between the devices and operate the TRNG in a region equivalent to a TRNG with upto 2% device mismatch. Since the output nodes of the TRNG are pre-charged to Vdd each cycle, the mismatch in pull down devices affect the behavior of the circuit more than the pull up transistors. Accordingly, the coarse calibration is also done using parallel stack of NMOS devices in both the inverters. By turning ON a specific set of these additional transistors, the TRNG can be made to operate in a region very close to the ideal situation, where each of bit 0 and bit 1 are generated with an equal probability. This is depicted in

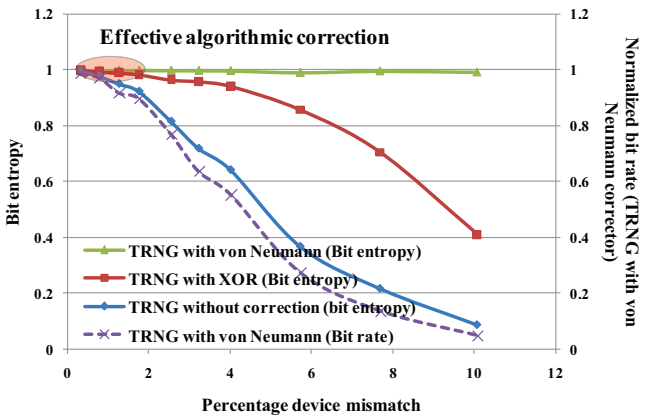

Figure 5: Bit entropy of TRNG without hybrid self-calibration

fig. 6. The output of the TRNG is monitored by a control logic that adaptively turns ON the configurable transistors to minimize the mismatch between the two pull down paths. Once coarse calibration is done, the TRNG operates in the highlighted region, close to the ideal scenario.

The control logic, fig. 7, comprises of a state machine that continuously monitors the output of the TRNG. If the initial output (at node b) of the TRNG is bit '0', the pull down in the inverter INV_1 is assumed to be stronger than that of INV_2. The control logic hence increments the configuration counter of INV_2 to increase the strength of the pull down path. The process continues till the output of the TRNG flips. Once the bit flips, a similar calibration is done till the bit flips again. The second iteration of tuning is performed to avoid any over-calibration. At this point, the TRNG is compensated for the coarse static mismatch due to intra-die variation and the self-calibration process stops.

Once the coarse calibration is performed, the output of the TRNG can be further processed using algorithmic techniques like XOR or von Neumann corrector, as shown in fig. 8. Feeding these entropy extractors with a calibrated TRNG instead of a raw biased TRNG helps in enhancing the

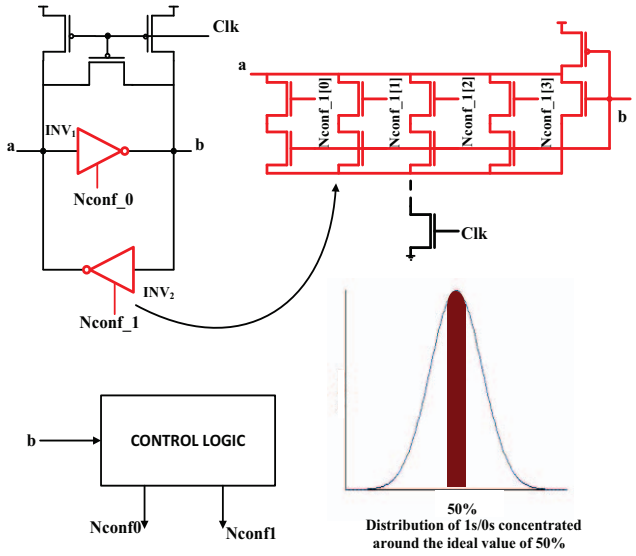

Figure 6: Coarse circuit calibration

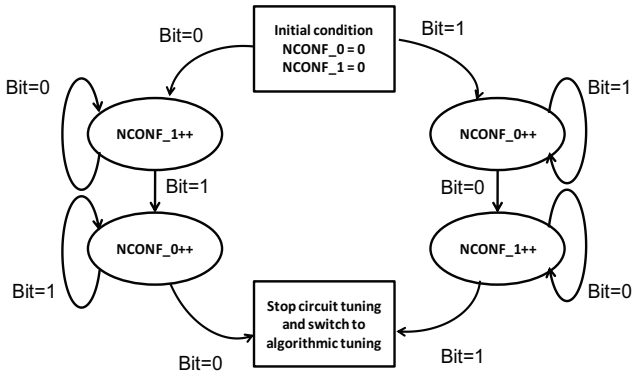

Figure 7: State machine for control of circuit calibration

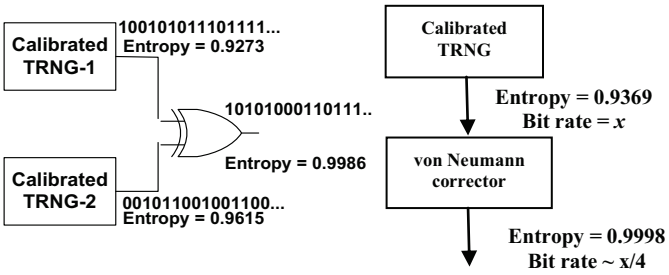

Figure 8: Algorithmic post-processing

bit entropy significantly for a larger range of device mismatch. The hybrid self-calibration technique uses adaptive circuit tuning only during the coarse calibration. Hence the control logic only contributes to the overhead in dynamic power only during the initial calibration step. Once the TRNG enters the algorithmic processing, the control logic is dormant and can even be powered down to negate the leakage. Algorithmic post-processing techniques rely on algorithm to extract entropy. They do not modify the TRNG circuit. Hence, they do not introduce any correlation between the bits. Further, algorithmic techniques are proven to be highly energy efficient and hence lead to a smaller overhead in terms of power.

5. Experimental setup and results

The proposed TRNG design using sub-Vdd pre-charge and hybrid self-calibration is validated using HSPICE simulations. The circuit is designed using the 45nm NCSU PDK. The transistor parameters are varied with a Gaussian distribution of $3\sigma = \pm 5\%$ with respect to the global variation, using the GAUSS function in HSPICE. The thermal noise is modeled as a random ΔV on the pre-charge voltage. The calculation of bit entropy and the automation of the flow are performed through a Perl based simulation platform. The circuit is simulated to generate 1Gbps.

5.1 Sub-Vdd pre-charge for TRNG

For a metastability based TRNG, the differential thermal noise at the two pre-charged nodes decide the output state. For instance, a TRNG biased (at node b, fig. 1) to 0 with P(0)=0.7 and P(1) = 0.3 implies that the pull down transistor N_1 is faster than N_2 or the current $I_{d1} > I_{d2}$. The output is resolved to a '1' only when the differential thermal noise

ΔV=V(b)-V(a) is large enough to overcome the mismatch and induce a scenario where $I_{d2} > I_{d1}$. Hence, fig. 4 also indicates the differential thermal noise required by the TRNG to overcome the mismatch and generate a random bit, for varying device mismatch and pre-charge voltage. Assuming that the thermal noise at the nodes 'a' and 'b' are independent and each have a Gaussian distribution with mean μ_{noise} and a variance σ_{noise}, the differential noise also has Gaussian distribution with mean '0' and variance $2\sigma_{noise}$.Hence, a smaller differential noise occurs with a greater probability as compared to a large differential noise, fig. 9. A plot of the probabilities of differential thermal noise required to compensate the device mismatch in the TRNG is shown in fig. 10. It is clear that the probability of differential noise required to nullify the intra-die variation is higher when the pre-charge voltage is lower. For a 2% device mismatch, the probability of the differential thermal voltage to compensate the variation at 0.7V pre-charge is ~2X the probability in case of 1.1V (Vdd) pre-charge. Thus, for a TRNG biased to '1', the probability of the output node resolving to a '0' increases with decreasing pre-charge voltage. In other words, the randomness of the TRNG increases for lower pre-charge voltages.

The pre-charge circuit is designed using pull down load on the pre-charge paths as shown in fig. 11 . Either NMOS or PMOS devices can be used to reduce the pre-charge from the nominal Vdd value of '1.1V'. Based on the device used, different amounts of reduction in pre-charge are obtained. Fig. 12 shows the voltage drop obtained due to NMOS and PMOS pull down devices of different sizes.

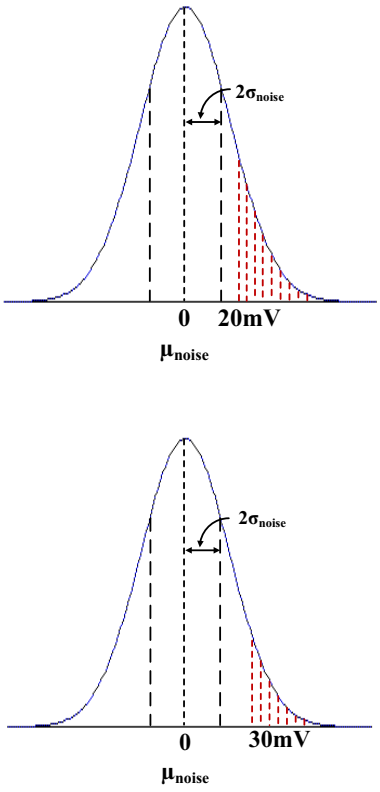

Figure 9: Distribution of random differential thermal noise

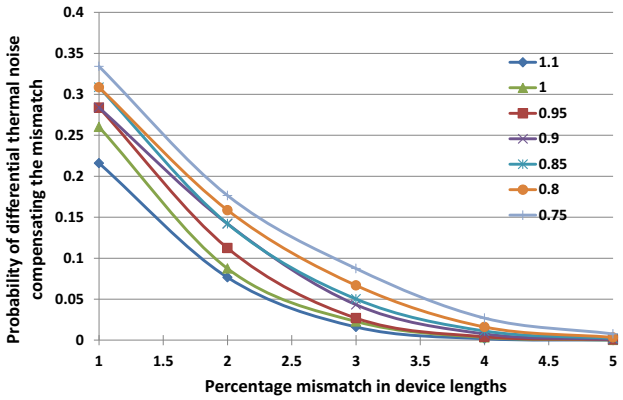

Figure 10: Probability of differential thermal noise required to overcome TRNG bias

For a constant device width, NMOS load provides larger drop and hence a lower pre-charge voltage as compared to PMOS. A 0.25u wide NMOS device can pull down the pre-charge voltage of 1.1 by ~400mV. This creates an effective pre-charge voltage of 0.7V instead of Vdd (1.1V). Hence, NMOS load is used to provide a coarse control of the pre-charge voltage, while the PMOS devices can be used for finer control. The loads on the pre-charged nodes are controlled by the clock signals. As a result the load is active only during the duration of pre-charge and is turned OFF when the TRNG evaluates the state. This reduces short circuit leakage and also does not have any impact on the resolution of stable state of the TRNG.

The above results indicate that operating the TRNG at a lower pre-charge voltage should improve the randomness and hence the entropy of the bits generated. Fig. 13 shows the plot of bit entropy of the TRNG with varying device mismatch for different pre-charge voltages. With increasing device mismatch, operating the TRNG with a lower pre-charge voltage results in better entropy. This makes the TRNG more tolerant to process variation. Since only the pre-charge voltage is reduced and not the supply voltage, there is no impact on the performance of the TRNG.

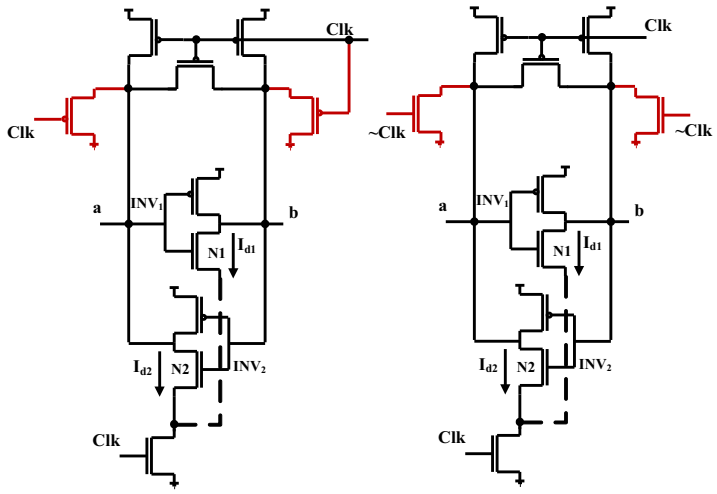

Figure 11: Circuit to generate sub-vdd pre-charge voltage

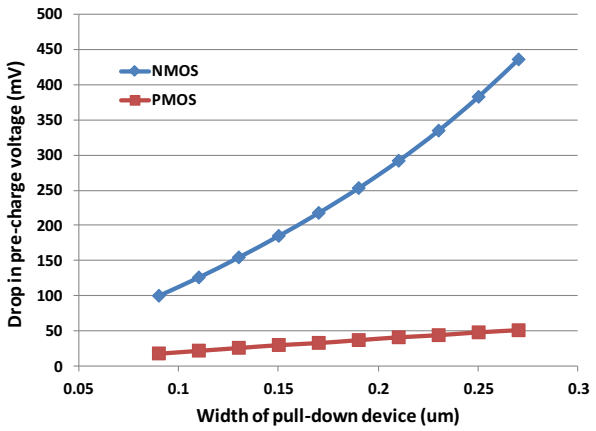

Figure 12: Effect of NMOS and PMOS load on pre-charge nodes

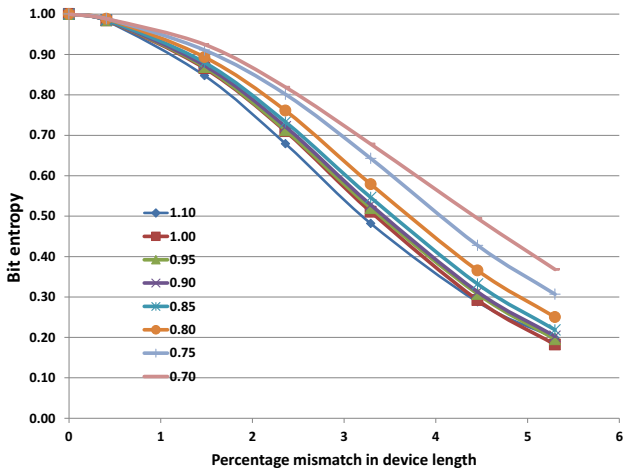

Figure 13: Bit entropy with increasing device mismatch and varying pre-charge voltage

5.2 Hybrid self-calibration

Although lower pre-charge voltage improves the tolerance of the TRNG to process variation, The entropy values obtained still do not qualify the TRNG to be used for cryptographic applications. Hence the TRNG is corrected using the hybrid self-calibration technique. The TRNG is initially calibrated to compensate for all coarse mismatch using the parallel NMOS stacks on the pull-down path of the two inverters. The control logic constitutes an area overhead of 128um2 which is ~50% of the TRNG area, owing to the significantly small design of the TRNG. Since the control logic is only active during the initial circuit calibration, it only accounts to the static power over a large period of circuit calibration. The energy overhead due to the adaptive control is a negligible 0.82fJ/bit.

The XOR function based hybrid self-calibration generates bit with a bit entropy close to the ideal value of '1'. Fig. 14 shows the variation of bit entropy with increasing device mismatch. A comparison with the initial result in fig. 5 shows that the value of entropy has increased by ~120% for upto 5% device mismatch. The plot also shows the entropy values and the trend line for pre-charge voltages of 0.7V and 1.1V. The results indicate that using a lower pre-charge value further improves the efficiency of the hybrid self-calibration technique.

The TRNG was also analyzed for hybrid self-calibration using the von Neumann correction. The von Neumann corrector, in theory discards the deterministic bits and just allows the random bits to pass through to the output. Hence, the output of a von Neumann corrector is always ~1 even for a highly biased TRNG. But, this correction is done at the expense of bit-rate. Fig. 5 indicates the decrease in bit rate of the von Neumann corrector with increasing device mismatch. Fig. 15 shows the plot of bit-rate at the output of the von Neumann corrector after hybrid self-calibration. Again, the results are further enhanced by the use of a lower pre-charge voltage.

6. Conclusion and future work

In this work we present a robust metastability based True Random Number Generator (TRNG) design with sub-Vdd

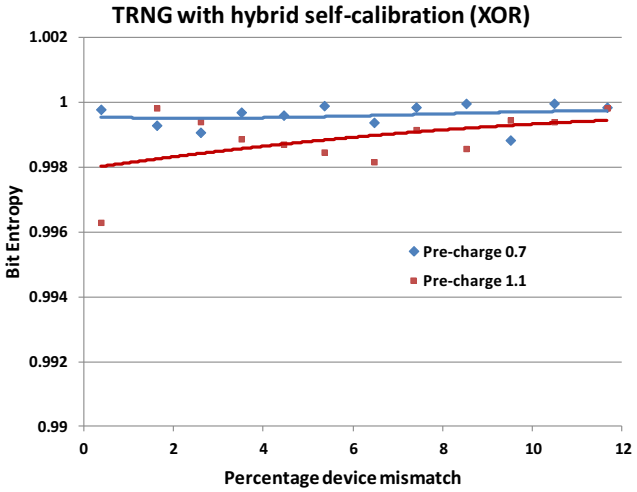

Figure 14: Bit entropy with hybrid self-calibration (XOR function)

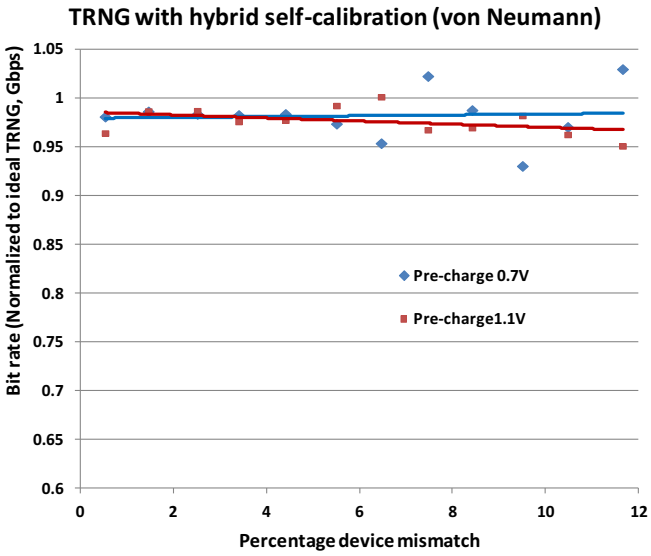

Figure 15: Bit entropy with hybrid self-calibration (von Neumann correction)

pre-charge and hybrid self-calibration technique. With increasing process variation, the statistics of TRNG gets degraded. Operating the TRNG with a lower pre-charge voltage makes it more tolerant to device mismatch. Reducing the pre-charge voltage by 40mV below nominal Vdd of 1.1V improves the randomness by ~2X. The entropy of the TRNG is further improved by using a combination of coarse circuit calibration followed by algorithmic post-processing. The proposed hybrid self-calibration technique works efficiently for intra-die variations as large as 5%, improving the bit entropy by ~120%. The proposed technique provides a practical design approach for robust random number generators in nanometer CMOS technologies. The sub-vdd pre-charge technique can be extended to an adaptive mechanism to choose the pre-charge voltage based on the post-Si entropy measurement.

9. 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," IEEE International Test Conference, 2008. ITC 2008

[9] A. Choudhary and S. Kundu, "A Process Variation Tolerant Self-Compensating Sense Amplifier Design," in IEEE Computer Society Annual Symposium on VLSI, 2009. ISVLSI '09, 2009, pp. 263-267.

[10] 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.

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

[12] 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

[13] T Markettos and S Moore, "The Frequency Injection Attack on Ring Oscillator based True Random Number Generators", CHES 2009.

[14] Wei Chen et al., "A 1.04 μW Truly Random Number Generator for Gen2 RFID tag," in *Solid-State Circuits Conference, 2009. A-SSCC 2009. IEEE Asian*, 2009, pp. 117-120.

[15] 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.

[16] C. Pyo, S. Pae, and G. Lee, "DRAM as source of randomness," *Electronics Letters*, vol. 45, no. 1, pp. 26-27, Jan. 2009.

[17] C. Tokunaga, D. Blaauw, and T. Mudge, "True Random Number Generator With a Metastability-Based Quality Control," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 1, pp. 78-85, Jan. 2008.

[19] 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.

[18] 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.

[20] 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.

[21] BSIM4v4.7 MOSFET Model: http://www-device.eecs.berkeley.edu/~bsim3/BSIM4/BSIM470/BSIM470_Manual.pdf

[22] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications: http://csrc.nist.gov/groups/ST/toolkit/rng/index.html