On-Chip True Random Number Generation in Nanometer Cmos

ON-CHIP TRUE RANDOM NUMBER GENERATION IN NANOMETER CMOS

A Thesis Presented

by

VIKRAM BELUR SURESH

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL AND COMPUTER ENGINEERING

February 2012

Department of Electrical and Computer Engineering

ON-CHIP TRUE RANDOM NUMBER GENERATION IN NANOMETER CMOS

A Thesis Presented

by

VIKRAM BELUR SURESH

Approved as to style and content by:

_____
Wayne P. Burleson, Chair

_____
Sandip Kundu, Member

_____ _____
Dennis Goeckel, Member

_____
C.V. Hollot, Department Head
Department of Electrical and Computer Engineering

ABSTRACT

ON-CHIP TRUE RANDOM NUMBER GENERATION IN NANOMETER CMOS

February 2012

VIKRAM BELUR SURESH

B.E, VISHVESHWARIAH TECHNOLOGICAL UNIVERSITY

M.S.E.C.E., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Wayne Burleson

On-chip True Random Number Generator (TRNG) forms an integral part of a number of cryptographic systems in multi-core processors, communication networks and RFID. TRNG provides random keys, device id and seed for Pseudo Random Number Generators (PRNG). These circuits, harnessing physical random variations like thermal noise or stray electromagnetic waves are ideally expected to generate random bits with very high entropy and zero correlation. But, progression to advance semiconductor manufacturing processes has brought about various challenges in the design of TRNG. Increasing variations in the fabrication process and the sensitivity of transistors to operating conditions like temperature and supply voltage have significant effect on the efficiency of TRNG designed in sub-micron technologies.

Poorly designed random number generators also provide an avenue for attackers to break the security of a cryptographic system. Process variation and operating conditions may be used as effective tools of attack against TRNG. This work makes a comprehensive study of the effect of process variation on metastability-based TRNG designed in deep sub-micron technology. Furthermore, the effect of operating temperature and the supply voltage on the performance of TRNG is also analyzed. To mitigate these issues we study entropy extraction mechanisms based both on algorithmic approach and circuit tuning and compare these techniques based on their tolerance to process variation and the energy overhead for correction. We combine the two

approaches to efficiently perform self-calibration, using a hybrid of algorithmic correction and circuit tuning to compensate the effect of variations. The proposed technique provides a fair trade-off between the degree of entropy extraction and the overhead in terms of area and energy, introducing minimal correlation in the output of the TRNG. Besides the study of the effect of process variation and operating conditions on the TRNG, we also propose to study the possible attack models on a TRNG. Finally, we propose a probabilistic approach to design and analysis of TRNG using a stochastic model of the circuit operation and incorporating the random source in thermal noise.

All analysis is done for 45nm technology using the NCSU PDK transistor models. The simulation platform is developed using HSPICE and a Perl based automation flow.

TABLE OF CONTENTS

Page

LIST OF TABLES……..….vii

LIST OF FIGURES……..ix

CHAPTER

1. INTRODUCTION 1

1.1 Ring Oscillator Based TRNG……..3

1.2 Metastability based TRNG……..4

2. EFFECT OF PROCESS VARIATION AND MITIGATION TECHNIQUES 7

2.1 Effect of process variation on TRNG……8

2.2 Entropy extraction using algorithmic post-processing……..10

2.3 Entropy extraction using circuit calibration……..12

2.4 Comparison of entropy extraction techniques……...14

3. EFFECT OF TEMPERATURE ON TRNG ..... …….20

3.1 Effect of temperature on MOS transistor…….20

3.2 Effect of temperature on MOS transistor in the presence of process variation……22

3.3 Effect of temperature on TRNG……...24

3.4 Effect of power supply noise on the behavior of the TRNG……26

4. SUB-VDD PRECHARGE TECHNIQUE 28

4.1 Effect of pre-charge on TRNG bias…….….28

4.2 Effect of process variation on TRNG offset voltage…….……31

4.3 Implementation and results with sub-vdd pre-charge……...34

5. HYBRID SELF-CALIBRATION TECHNIQUE FOR ENTROPY EXTRACTION 37

5.1 Proposed hybrid self-calibration technique……..38

5.2 Implementation and Results…….……41

5.3 Hybrid self-calibration with sub-vdd pre-charge……..44
6. ATTACK MODELS FOR TRNG 47
6.1 Process variation ……..48
6.2 Operating temperature……..49
6.3 Varying Supply voltage……51
6.3.1 Detection of attack……...54
6.3.2 Prevention of attack: Asymmetric duty cycle……..…...55
6.4 Varying duty cycle of clock……..56
6.5 Crosstalk……57
7. STOCHASTIC MODEL FOR METASTABILITY BASED TRNG 60
7.1 Thermal Noise in an isolated NMOS transistor……..60
7.2 Probabilistic analysis of Metastability based TRNG……..62
7.4 Analysis of post-processing techniques……..68
7.4.1 XOR Function……68
7.4.2 von Neumann corrector……...69
7.5 Implementation and Results……70
8. CONCLUSIONS 75
APPENDIX: SIMULATION ENVIRONMENT 76
BIBLIOGRAPHY..... 79

LIST OF TABLES

Table Page

1. von Neumann function for entropy extraction 11

2.Bit entropy of TRNG using XOR function for correction [15] 15

3. Energy/bit for different entropy extraction techniques [15] 17

4. variation of byte entropy with increase in temperature 51

5: Variation of byte-entropy with bit-entropy 58

6: Key space with varying bit entropy 59

LIST OF FIGURES

Figure Page

1. Basic TRNG system 2

2. Ring oscillator based TRNG 3

3. Metastability based TRNG 5

4. Variation of bit entropy with device mismatch [15] 9

5. TRNG with algorithmic post-processing 10

6. TRNG using XOR function for post-processing 11

7. Variable bit rate due to von Neumann correction 12

8. Entropy extraction using von Neumann corrector 12

9. Metastability-based TRNG 13

10. Coarse grain calibration [14] 13

11. Fine grain calibration [14] 14

12. Variation of bit entropy using von Neumann corrector [15] 15

13. Variation of bit rate and energy consumption of von Neumann corrector [15] 16

14. Comparison of the bias removal techniques [15] 17

15. Variation of bit entropy and energy/bit for varying number of configuration bits [15] 18

16. Variation of NMOS drain current with temperature 21

17. Variation of drain current of NMOS of different channel length with increase in temperature 23

18: Rate of decrease in drain current for different values of device mismatch 24

19: Hamming distance compared with TRNG at $0^{o}C$ 25

20: Hamming distance compared with TRNG at $0^{o}C$ 25

21: Variation of entropy with increase in temperature 26

22: Hamming distance of bits compared with TRNG with stable power supply 27

23: Cross-coupled inverters 29

24: Effect of increasing differential voltage on biased TRNG 31

25: Analysis of differential voltage to compensate mismatch 32

26: Distribution of thermal noise 33

27: Circuit to generate sub-vdd pre-charge voltage 35

28: Effect of NMOS and PMOS load on pre-charge nodes 35

29: Bit entropy with increasing device mismatch and varying pre-charge voltage 36

30: Effectiveness of algorithmic technique for smaller mismatch 39

31: Coarse circuit self-calibration 40

32: State machine for control of circuit calibration 40

33: Algorithmic post-processing for finer entropy extraction 41

34: Entropy extraction with hybrid self-calibration 42

35: Robustness of hybrid self-calibration against variation in temperature 43

36: Energy overhead with hybrid self-calibration (pre-charge = 1.1V) 44

37: Comparison of hybrid self-calibration with different pre-charge voltages (XOR function) 45

38: Comparison of hybrid self-calibration with different pre-charge voltages (von Neumann function) 45

39. Distribution of 8-bit key for ideal TRNG 48

40. Distribution of 8-bit key for TRNG with 2% device mismatch 49

41. Distribution of 8-bit key for TRNG with 2% device mismatch operating at 25^{o}C 50

42. Distribution of 8-bit key for TRNG with 2% device mismatch operating at 100^{o}C 50

43: Variation of evaluation time with differential noise 51

44: Variation of pre-charge and evaluation time with supply voltage 52

45: Variation of evaluation time with decreasing operating voltage 53

46: Erroneous bit due to reduced supply voltage 53

47: Variation of entropy with decreased power supply voltage 54

48: Voltage scaling attack prevention using asymmetric duty cycle clock 55

49: Bit entropy of TRNG with asymmetric duty cycle 56

50: Attack on TRNG by varying clock duty cycle 57

51. Distribution of 8-bit key for an ideal TRNG with crosstalk attack 58

52: TRNG circuit with pull down currents 62

53: Distribution of entropy with variation in length 67

54: Distribution of entropy for variation in L_{eff} 71

55: Weighted distribution of bit-entropy (3-sig Leff variation = 5%) 72

56: Weighted distribution of bit-entropy (3-sig Leff variation = 10%) 72

57: Expected entropy/bit rate with different sigma variation in process 73

58: Comparison of stochastic model with HSPICE simulation 74

59. TRNG circuit extracting randomness from thermal noise 77

60. TRNG circuit modelled in spice with varied pre-charge to mimic the effect of thermal noise 77

61. HSPICE and PERL based simulation platform for study of TRNG 78

CHAPTER 1

INTRODUCTION

Secure processing, communication and data transfer have been major areas of research and development over the last decade. A number of applications ranging from complex processing and data communication to light-weight ubiquitous applications like smart cards and RFID depend on a secure environment for their operation. Numerous communication protocols and cryptographic algorithms have been developed in this direction. Most of these techniques depend on secure transfer of data based on authentication or data encryption. This has created a need for generation of random keys or id. Pseudo Random Number Generator (PRNG) is frequently used to generate random keys for these purposes. Since a PRNG is algorithm based, it is vulnerable to traditional crypto attacks as well as attacks based on Differential Power Analysis (DPA) and Electromagnetic emissions (EM). To secure the key generation, either the algorithm of the PRNG has to be designed to be more complex, adding to an overhead in the area and power of the design or the PRNG seeded using a more random source. Thus, the need for design of efficient and light weight True Random Number Generators (TRNG) is ever increasing in the field of secure computing.

TRNG is fundamentally a circuit that extracts randomness from a physical phenomenon having a random distribution. Unlike a PRNG, the state of a TRNG is independent of the previous states and generates bits with entropy very close to the ideal value of '1'. A basic TRNG circuit would consist of three components, as shown in figure 1, the source of randomness, the extraction circuit and the post-processing unit. Cosmic rays, stray electromagnetic waves and thermal noise are some of the potential sources of randomness. A TRNG samples and digitizes these continuous sources to extract the randomness. The entropy may be extracted in the form of random clock jitter samples, power up state of memory cells, meta-stability of devices and chaos on deterministic analog signals. Due to imperfections in the source of entropy or the sample and digitize circuit, the output of the TRNG may not have the preferred degree of randomness.

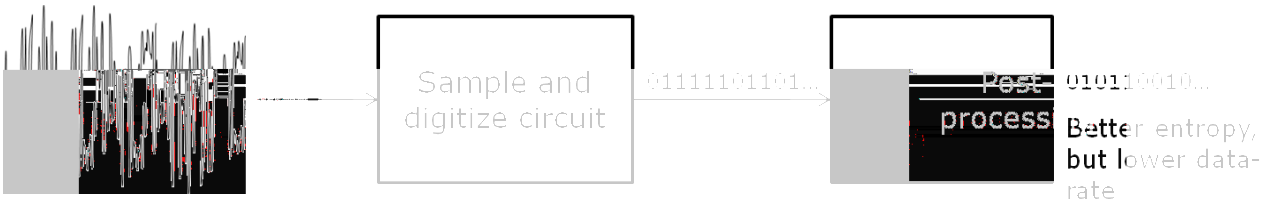


Figure 1. Basic TRNG system

To improve the randomness and further extract entropy, various post-processing techniques are employed. On-chip TRNG circuits are being increasingly used in various applications to enhance the security. "Ultra-wide band for Low Power Security", our exploratory project funded by the National Science Foundation, explores the application of TRNG to low power security.

Various sample and digitize circuits have been discussed in literature to extract entropy from a random source. Optical designs have been developed to monitor the behavior of a single photon in free space. This information is sampled using a discrete digital circuit to extract random bits [1]. A Geiger –Mueller tube is used to detect individual radioactive disintegration. The decay rate of atoms of radioactive material can be sampled to generate random data. Johnson noise across a resistor can be used as a source of randomness. The amplified thermal noise is fed to a voltage controlled oscillator, the output of which is sampled to obtain random bits [2]. Memory based designs can also be used as TRNG. The random access time in DRAM due to collision between the memory access and the refresh cycles serve as a source of entropy [3]. Ring oscillator based TRNG and metastability-based TRNG are the most commonly used digital designs for on-chip random number generation since these circuits directly provide a digitized output. These circuits will be discussed in the following sections.

1.1 Ring Oscillator based TRNG

Jitter in Ring Oscillators (RO) provides a simple and effective way to extract randomness. RO based TRNG are popular as they can be implemented efficiently in both ASIC/custom as well as FPGA based designs [4][5][6][7]. A ring oscillator is built using an odd number of inverters and feeding back the output of final inverter to the input of first inverter. Variation in power supply in the form of IR drop or supply noise causes a variation in the inverter delays and hence the frequency of oscillation. This uncertainty of the oscillator signal (output) in time domain is termed as Jitter. Since the jitter depends on various factors, some of which are random, it can be used as a source of randomness in the design of an RO based TRNG. The basic TRNG circuits use two or more ring oscillators as shown in figure 2 and XOR the outputs. The output signal of the XOR is sampled during the transition zone to get random values because of the jitter in the two oscillator rings.

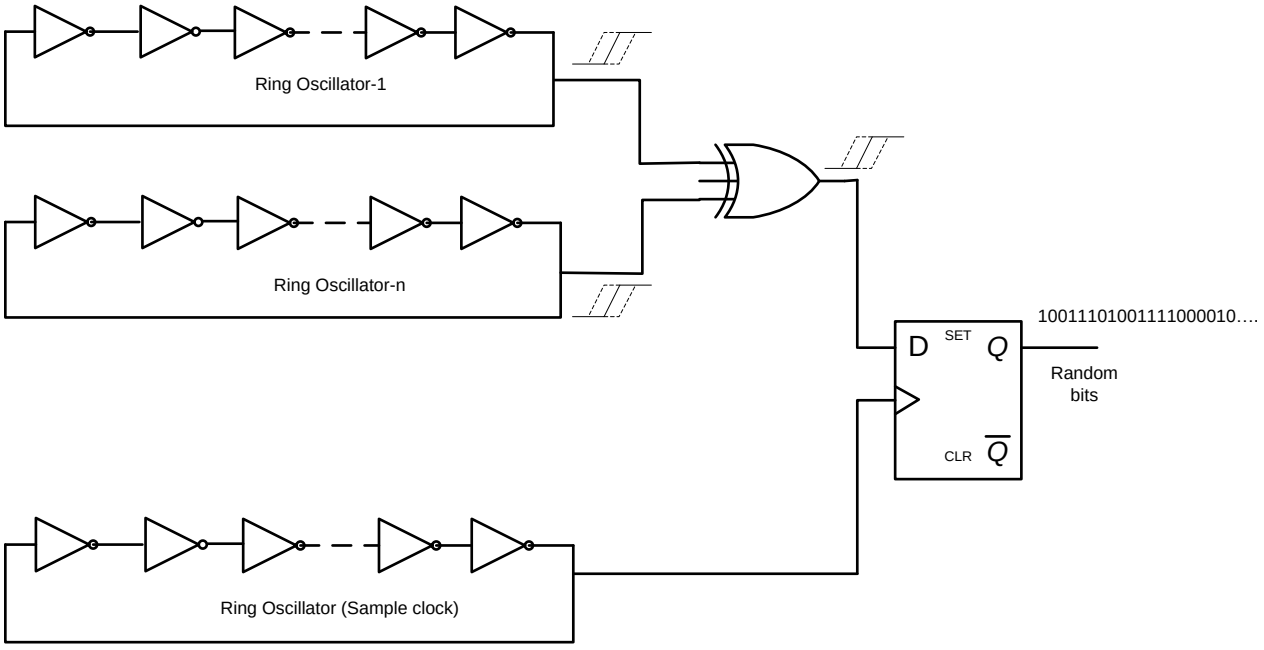


Figure 2. Ring oscillator based TRNG

A number of variations of this idea have been discussed in literature. The output of a faster RO when sampled by a slower RO, whose jitter is comparable to the period of the faster clock, generates random bits [8]. The outputs of a number of ring oscillators can be combined using an XOR gate and sampled to obtain a stream of random bits. The output of the XOR gate will have a spectrum of transitions, some deterministic and some random. The deterministic transitions are caused due to the overlap of jitter between the ring oscillators. The TRNG system is designed in such a way as to fill the spectrum with a large number of random transitions and sample the same using an appropriate sampling signal [4]. One approach is to use oscillator rings of variable lengths. When two rings of relatively prime length, generating clock signals of period 2T, 3T and so on are used, they produce a random transition at time instants equal to common multiples, which in this case is 6T, 12T, 18T, etc. By filling up the spectrum with such transitions using more than two oscillator rings and sampling the data only at such time instants produces a stream of random bits. Yet another form of RO based TRNG consists of a counter clocked by the output of a ring oscillator. The counter value sampled after a number of cycles of a reference clock, can be expected to give different values in different samples based on the random jitter in the ring oscillator [5].

1.2 Metastability based TRNG

Metastability based TRNG circuits are based on metastable circuit elements like cross-couple inverters or SRAM cells to extract randomness from thermal noise. On-chip SRAM memory provides a very convenient technique for generating random numbers. During the power up process, the SRAM cells restore to a stable state of either a '0' or a '1' based on the random thermal noise present in the design, providing random bits [9]. Similarly, when both the outputs of a cross coupled inverter pair is charged to Vdd or logic '1', the inverters are driven to a metastable state. Upon releasing the charge, the inverters take some time to restore to a stable state. The resolution time is a function of the thermal noise present and can be used to generate

random bits [10]. In modern cryptographic applications, metastability based TRNG are being increasingly used since they are simpler to design, in some cases making use of the already available hardware and consume less energy as compared to other TRNG circuits. Thus in this work we focus mainly on efficiency of metastability based TRNG and the effect of process variation and operating conditions on these circuits.

A basic metastability based TRNG, considered for this work, consists of a pair of cross coupled inverters, figure 3. The inputs of both the inverters are pre-charged to logic HIGH, through two PMOS transistors during the negative half cycle of the clock. Thus, both the inverters are driven to a metastable state. During the positive half of the clock cycle, the pre-charge is removed and then inverters are allowed to come out of the metastable state and settle down to a stable state. If both the inverters are identical in all respects, the random differential thermal noise at the inputs of the inverters decides the resolution state. Hence, under an unbiased

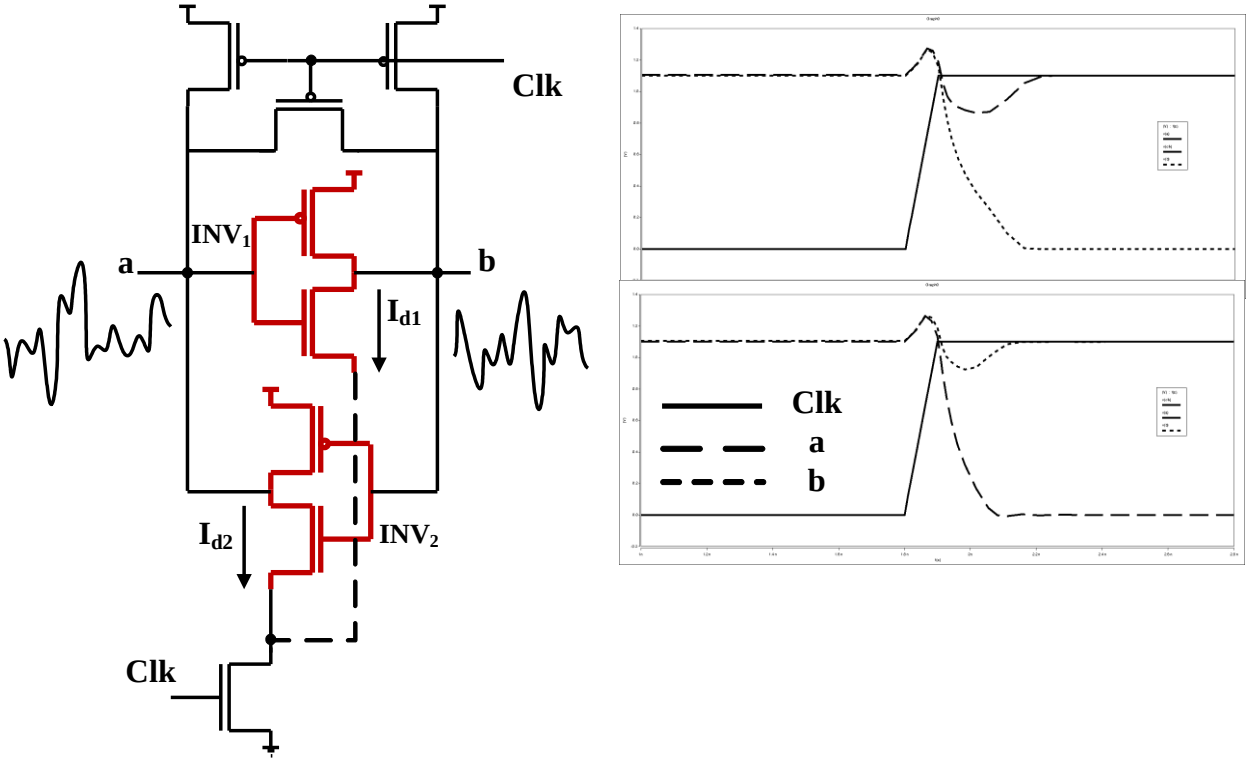


Figure 3. Metastability based TRNG

operating condition, thermal noise acts as the source of randomness to generate a bit '0' or a bit'1' at each cycle.

Under matched conditions, the circuit behaves as a fair coin generating bit '0' and bit '1' with an equal probability of 0.5, resulting in an ideal bit entropy of 1. But, in deep sub-micron technologies, increasing variation in process and changes in the operating conditions may impact the behavior of the TRNG. Thus, the effect of variation in the process, temperature and supply voltage and the analysis of circuits from a cryptographic perspective is an important topic of study in the field of design and security of on-chip random number generators.

CHAPTER 2

EFFECT OF PROCESS VARIATION AND MITIGATION TECHNIQUES

Process variation is undoubtedly the major challenge in the evolution of CMOS technology 45nm and below. Reducing feature sizes have imposed additional constraints on the design and fabrication methodology. The actual fabricated feature dimensions, transistor threshold voltages and the dopant concentrations are observed to vary more in terms of percentage, compared to the models used in the design phase, as we move to lower technology nodes. These factors affect the performance of the designs in terms of delay, power and reliability.

The variations in transistor behavior may be attributed to a number of factors. Random Dopant Fluctuation (RDF) is caused due to random variation in the dopant concentration in the transistors. With reducing channel lengths, the number of dopant atoms is decreasing exponentially. Hence, even a small variability in few random dopant atoms results in different electrical characteristics of two transistors fabricated one beside the other. With the advent of technology, the feature dimensions are decreasing at a faster rate compared to the wavelength of the light source used for optical lithography. In 45nm fabrication process, feature sizes as small as 45nm are fabricated using a light of wavelength 193nm. Thus each feature fabricated on the silicon is affected by the size, shape and density of the features surrounding it. The effect seen in the form of Line Edge Roughness (LER) and Line Width Roughness (LWR) has increased the intra-die variations. Also, variation in the oxide thickness leads to variation in the threshold voltage of different transistors on the same die. All these factors constitute the static variation that is observed during the fabrication process.

Apart from the fabrication process, a number of factors that vary dynamically during the functioning of the chip also affect the behavior of the transistors. Short channel effects like channel length modulation, electron-migration in interconnects, NBTI and other wear out effects

hamper the performance of deep sub-micron designs. The effect of both the static and dynamic variations may be modeled in the form of one of the following parameters:

1. Variation in transistor length (Effective length of the channel)
2. Variation in transistor width
3. Variation in threshold voltage

One or more of these variations may impact the other parameters as well. Of these, the variation in transistor length has the most significant effect on the behavior of the transistor.

2.1 Effect of process variation on TRNG

Variation in process affects the delay and power of a transistor. But, from a cryptographic point of view, it is more important to analyze how these effects translate into variation in the randomness of the TRNG. Under ideal conditions, the TRNG acts as a fair coin. The generation of bits is solely dependent on the random differential thermal noise at the inputs of the two inverters. But, a relative variation in the feature size or threshold voltage of the transistors in the cross coupled inverters would lead to a bias in the circuit. Based on the mismatch, one of the inverters will tend to be faster than the other, resulting in more zeros/ones generated at its output as compared to the other. Unless the differential noise is strong enough to overcome this mismatch, the TRNG would generate an output biased to either '1' or '0'. So, the probability of the bits generated will deviate from the ideal value of 0.5, reducing the bit entropy below 1.

The degree of randomness of the bits generated by a RNG is evaluated through various statistical tests developed by organizations like the National Institutes of Standards and Technology (NIST) [11]. The NIST suite consists of a series of tests that focus on a variety of different types of non-randomness that could exist in a sequence. Although the NIST tests are necessary for validating a TRNG, the bit entropy of a sequence of bits generated, provides a reasonable idea of the lack of randomness. The bit entropy $H(X)$ is given by the following equation:

$$\boldsymbol{H(X) = -p(1)\log_2[p(1)] - p(0)\log_2[p(0)]} \qquad \boldsymbol{(2.1)}$$

$$where\ p(1) = probability\ of\ bit\ '1'$$

$$and\ p(0) = probability\ of\ bit\ '0'$$

Hence, in the following work, bit entropy is used to analyze the effect of process variation on the TRNG.

The Metastability-based TRNG circuit discussed in the previous chapter was modeled in HSPICE. Since the variation in the transistor length has the most significant effect on the electrical behavior, Monte-Carlo simulations were performed for a relative 3-σ variation of 20% between the transistor lengths of the two inverters in the design.

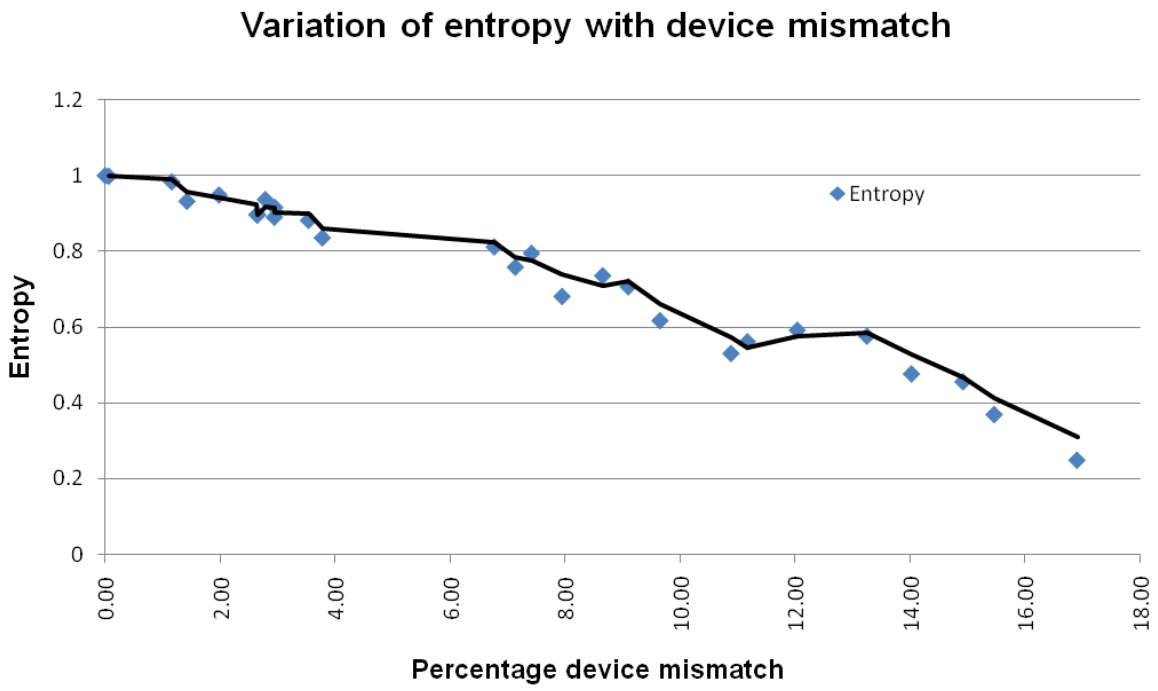


Figure 4. Variation of bit entropy with device mismatch [15]

The results, as shown in figure 4, indicates that the bit entropy of the TRNG output decreases with increasing device mismatch. Thus, the TRNG cannot be effective for

cryptographic applications when used stand alone. Correction mechanisms have to be employed to extract additional entropy. The correction mechanism may be a traditional algorithmic post-processing or tuning the circuit to compensate for the mismatch. Each of these approaches presents trade-off between the energy overhead for correction and the degree of correction achieved.

2.2 Entropy extraction using algorithmic post-processing

The entropy of the bits generated by a TRNG may be improved using a number of algorithmic approaches, figure 5. XOR function is a very simple and commonly used correction technique [4]. von Neumann correction is another very efficient entropy extractor that is widely used in random number generation [2][4][8]. Apart from these, universal hash function [9] or Secure Hash Algorithm (SHA-1) are also used for improving the randomness of TRNG.

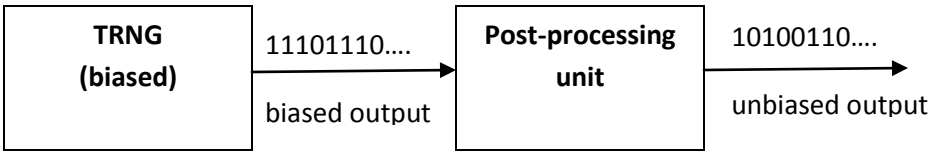


Figure 5. TRNG with algorithmic post-processing

XOR function:

The XOR function is a commonly used entropy extractor. When the outputs of two or more TRNG circuits are XORed to improve the entropy of the output as shown in figure 6, the bias in one of the circuits is masked by the other TRNG circuits. Although the XOR function provides a simple implementation for improving the entropy of the design, it leads to overhead in the form of multiple TRNG circuits to generate bits. From the law of averaging the implementation would produce better results as more number of TRNG circuits are used. But, this would lead to additional overhead in terms of area and power. Further, care should be taken

to place the circuits in close vicinity to avoid non common mode variation in the operating conditions.

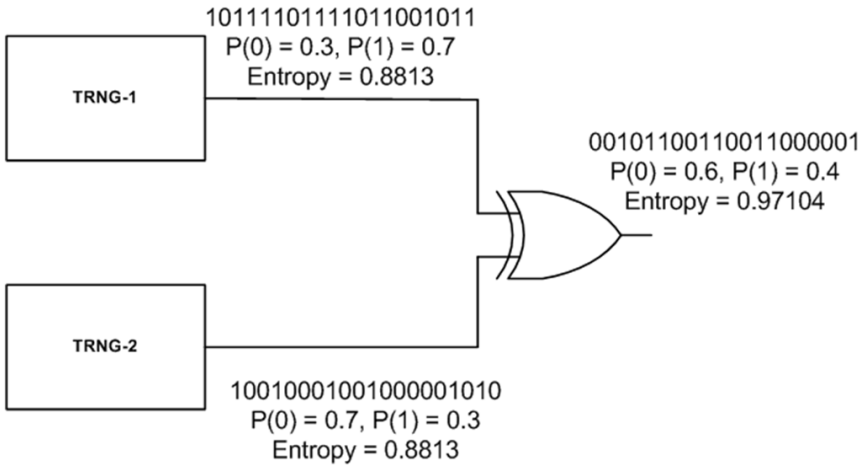


Figure 6. TRNG using XOR function for post-processing

von Neumann corrector:

The von Neumann corrector is the most widely used correction mechanism to enhance the entropy of a TRNG. The von Neumann function, as shown in table 1, generates a uniform distribution on bit '0' and bit '1'. It considers simultaneous pairs of bits from the TRNG. A bit '0' is generated if the TRNG bit sequence is [1,0] and a bit '1' is generated if the TRNG bit sequence is [0,1]. Bit sequences [0,0] and [1,1] are discarded.

Table 1. von Neumann function for entropy extraction

Input bit pairs (from TRNG)	Output from von Neumann Corrector
00	No output
01	1
10	0
11	No output

The von Neumann corrector provides significant improvement in the entropy by generating bits with entropy very close to the ideal value of 1. But, since some of the bit sequences from the TRNG are discarded, the output bit rate of the von Neumann is dependent on the TRNG output and hence not constant.

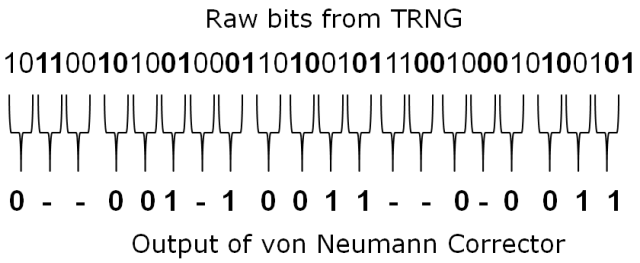


Figure 7. Variable bit rate due to von Neumann correction

Hence, a shift register has to be used to store the corrected bits and use it for further processing, figure 8. This adds to the area and power overhead.

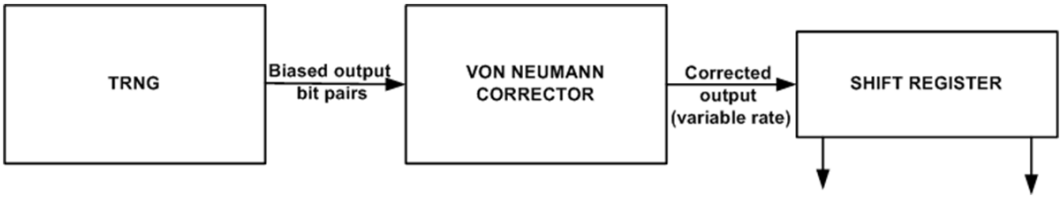


Figure 8. Entropy extraction using von Neumann corrector

2.3 Entropy extraction using circuit calibration

Circuit tuning mechanisms have been used in deep sub-micron technology for post fabrication clock skew and delay tuning. Digital de-skewing circuits have been used for clock distribution in microprocessor designs to mitigate variations and gradients to match the clock signal between two clusters [12]. Process monitoring circuits are used to detect variations and calibrate on-chip thermal sensors [13]. Charge injection is another way to compensate for mismatches in the circuit [10]. Similar circuit calibration techniques may also be extended to

TRNG design to compensate for device mismatch due to process variation. In a publication by Intel Corp. a two stage circuit calibration mechanism has been proposed a two stage circuit calibration mechanism to mitigate the effect of process variation, figure 9 [14].

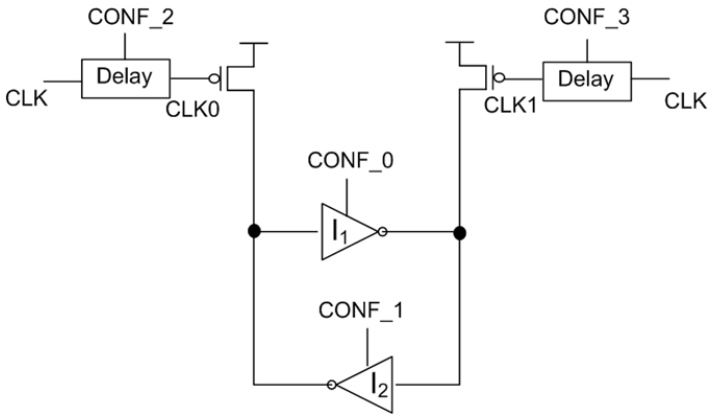


Figure 9. Metastability-based TRNG

The coarse grain calibration circuit, figure 10, consists of parallel PMOS and NMOS structures in both the inverters. These act as additional source and sink paths respectively to compensate for an increase in speed of the other inverter and hence match the two devices.

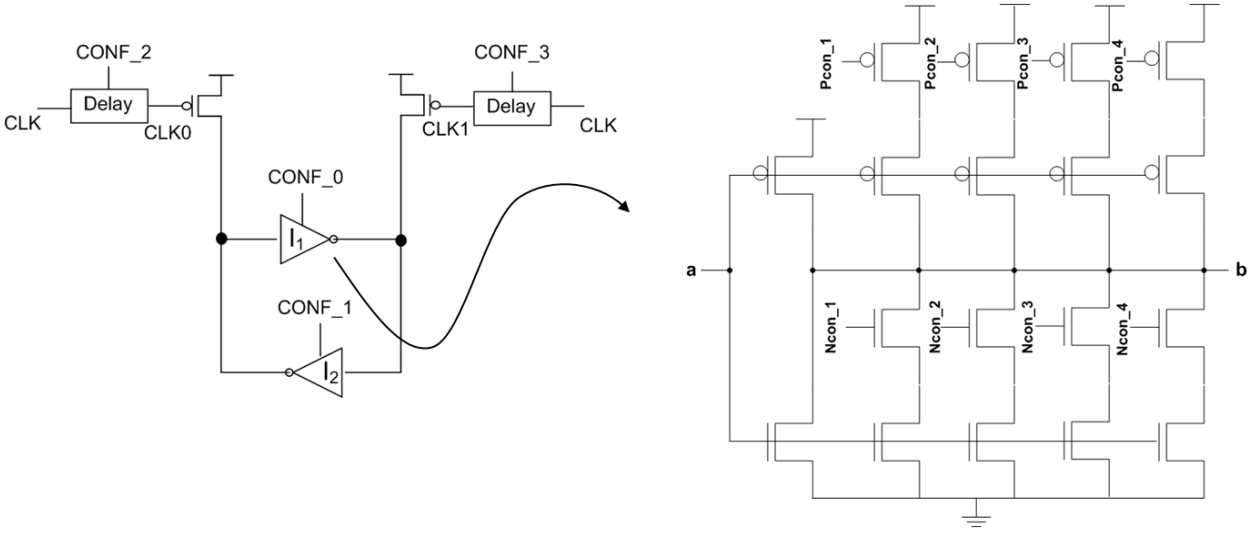


Figure 10. Coarse grain calibration [14]

The fine grain calibration, figure 11, provides a variable delay tuning mechanism for the pre-charge clock. By increasing the delay on the pre-charge clock path, either one of the inputs of the two inverters are held at logic ‘1’ for longer than the other, thereby compensating for the bias introduced due to device mismatch.

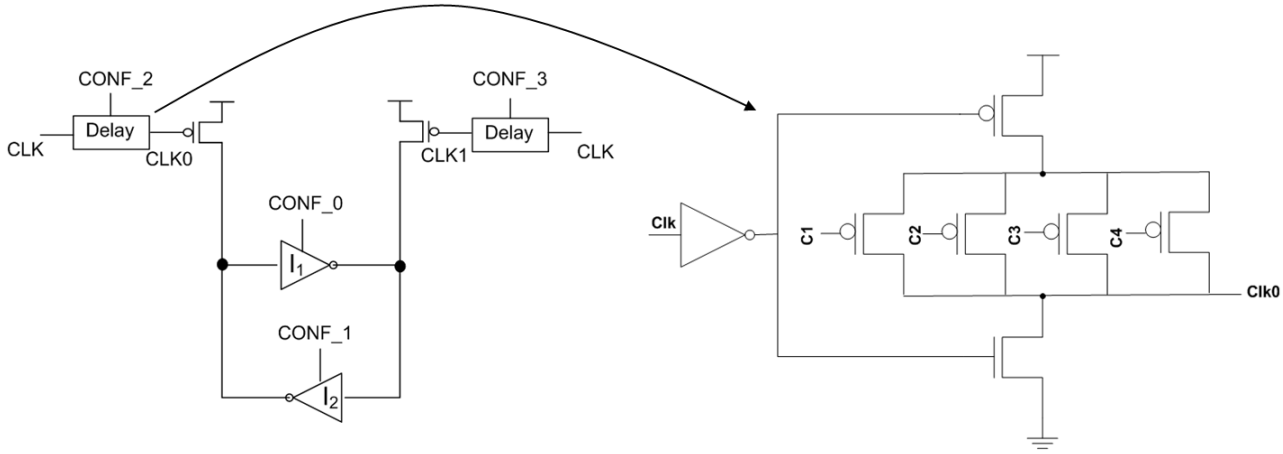


Figure 11. Fine grain calibration [14]

Once the TRNG is fabricated, bits can be generated during the chip testing process. Depending on the bit entropy, the bias in the TRNG due to process variation is estimated. Accordingly, appropriate configuration bits are set to perform a combination of coarse and fine grained tuning to compensate for the bias and achieve an entropy close to ‘1’.

2.4 Comparison of entropy extraction techniques

The different entropy extraction mechanisms were analyzed for the degree of improvement in randomness achieved for varying device mismatch [15].

The XOR function, as shown in table 2, provides considerable improvement in the entropy if one of the two TRNG used can generate bits with high entropy. But, as the device mismatch in both the inverters increase, there is minimal improvement in the entropy obtained through the XOR function. The bit entropy falls much below the value desired for cryptographic applications for any device mismatch more than 3%.

Table 2.Bit entropy of TRNG using XOR function for correction [15]

Iteration	% Device mismatch in TRNG-1	Entropy of TRNG-1	% Device mismatch in TRNG-2	Entropy of TRNG-2	Entropy of XOR output
1	2.79E+00	0.966	5.94E-02	0.986	0.998
2	7.79E+00	0.817	3.03E+00	0.945	0.988
3	3.83E+00	0.941	1.48E+00	0.971	0.973
4	1.20E+01	0.683	2.65E+00	0.786	0.931
5	4.06E+00	0.787	1.03E+01	0.597	0.881
6	1.34E+01	0.708	8.65E+00	0.555	0.847
7	1.55E+01	0.592	6.77E+00	0.699	0.82
8	7.95E+00	0.516	1.15E+01	0.678	0.814
9	1.49E+01	0.486	9.10E+00	0.682	0.81
10	1.23E+01	0.529	6.69E+00	0.663	0.777

von Neumann corrector provides a very significant improvement in the bit entropy. Since, consecutive zeros and ones are discarded by the algorithm, non-random bits are filtered and only the bit stream with high entropy is extracted.

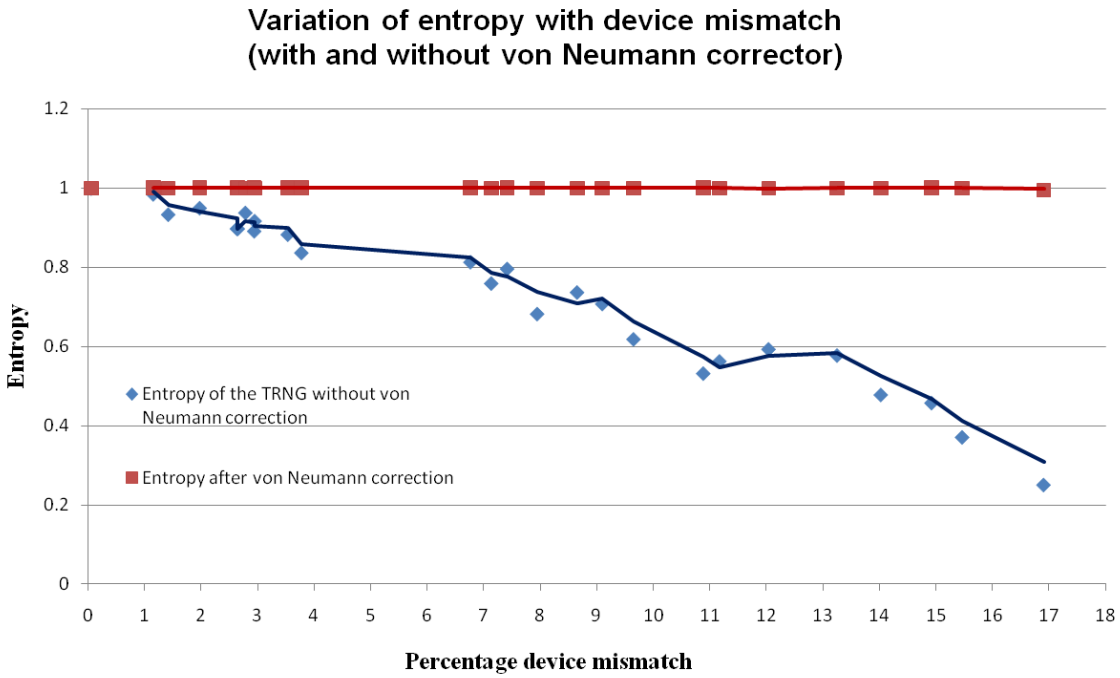


Figure 12. Variation of bit entropy using von Neumann corrector [15]

But, with increase in device mismatch, the TRNG will be biased to either '0' or '1'. Hence, it generates the sequences [0,0] or [1,1] more frequently. As a result more number of TRNG bits has to be generated per bit extracted from the corrector and the output bit rate of the von Neumann corrector decreases. This results in increased energy consumption per bit.

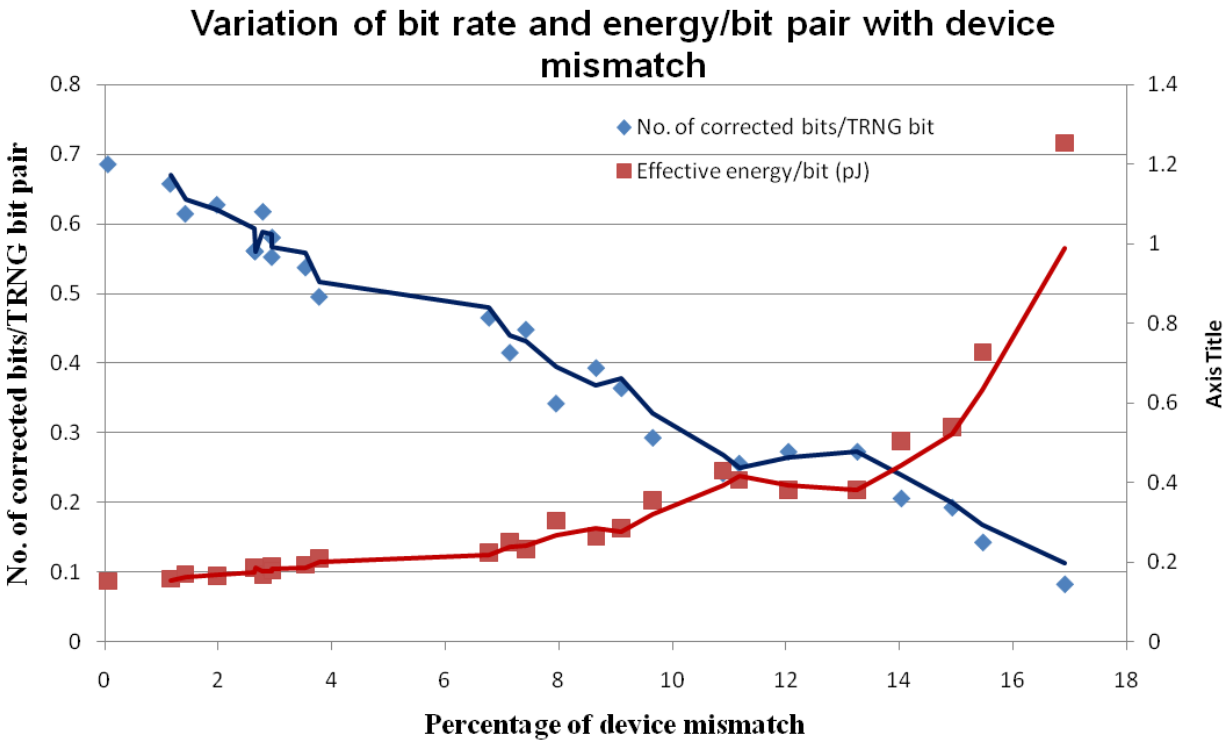


Figure 13. Variation of bit rate and energy consumption of von Neumann corrector [15]

The circuit calibration technique is seen to provide an improvement in the entropy comparable to the von Neumann corrector. A comparison of the bit entropy with varying device mismatch is as shown in figure 14.

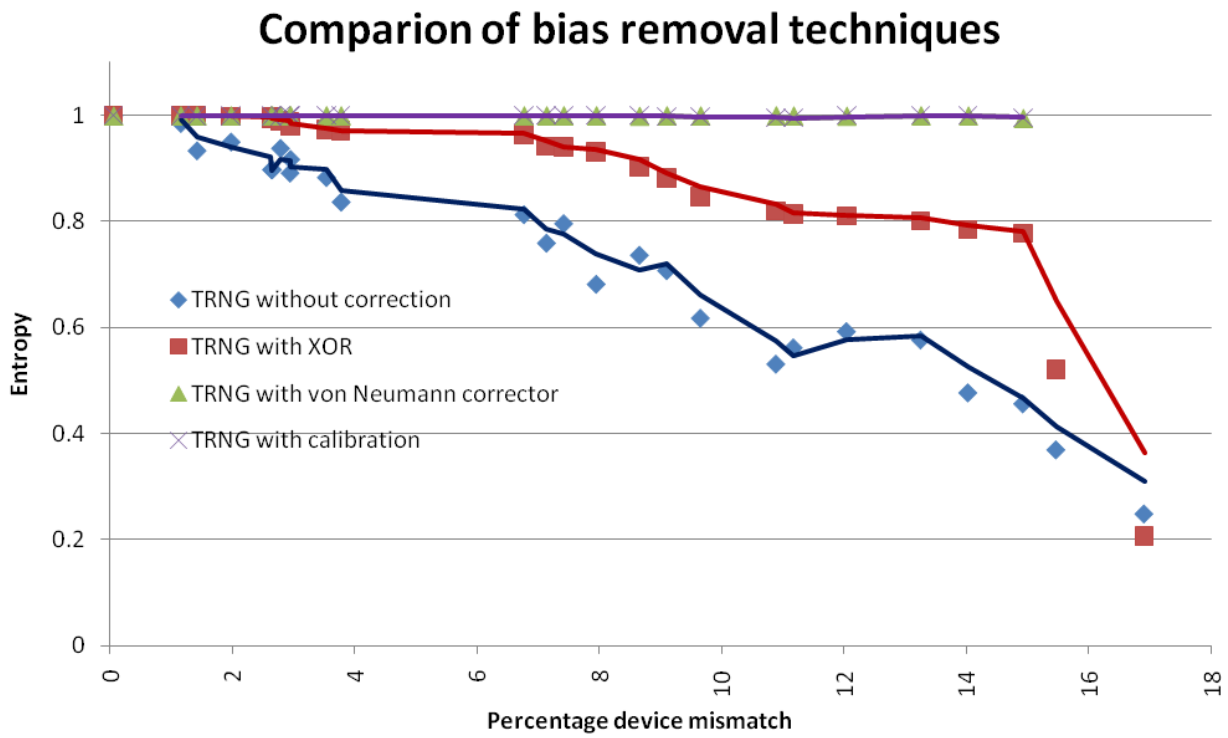


Figure 14. Comparison of the bias removal techniques [15]

Table 3. Energy/bit for different entropy extraction techniques [15]

Bias removal technique	Average Energy/Random bit (pJ)
TRNG without correction	0.001
TRNG with XOR function	0.006
TRNG with von Neumann Corrector	0.282
TRNG with calibration	0.124

An important trade-off in choosing the correction mechanism, especially for lightweight applications like RFID is the energy overhead per random bit. Table 3 summarizes the energy consumption per bit of the TRNG with each entropy extraction technique.

Although the XOR function adds to very little overhead in terms of energy, it proves to be inefficient for increased process variation. Even with a device mismatch of 3%, the bit entropy drops below the values expected for cryptographic applications. The von Neumann corrector generates bits with entropy very close to '1'. But, with increase in process variation, more bits have to be generated by the basic TRNG per bit extracted. As a result the energy per bit increases. The average energy per bit observed is 0.282pJ, with the maximum value crossing 1pJ/bit for variations greater than 15%.

The circuit calibration mechanism provides a good trade-off between the enhancement in randomness and the energy overhead. It is efficient for more than 12% larger variation as compared to the XOR function. It provides an entropy extraction comparable to that of the von Neumann corrector but at 56% lower energy overhead. The calibration technique also provides the flexibility of varying the number of configuration bits based on the variation expected in a process.

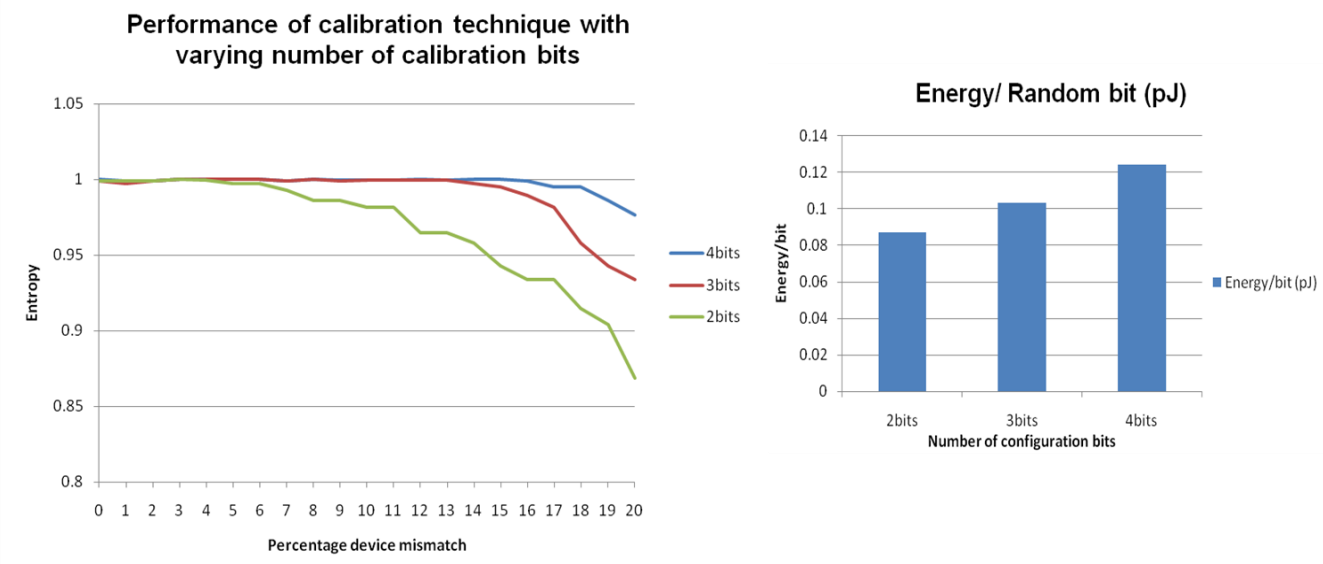


Figure 15. Variation of bit entropy and energy/bit for varying number of configuration bits [15]

With decreasing number of configuration bits, the calibration technique provides effective correction for lesser process variation. But, accordingly the energy overhead also reduces. Hence based on the expected process variation, fewer configuration bits may be used along with combination of algorithmic post-processing to achieve minimal energy overhead.

CHAPTER 3

EFFECT OF TEMPERATURE ON TRNG

Post fabrication, the operating conditions of the chip also affects the behavior of CMOS circuits. Variation in temperature and supply voltage impacts the delay of the transistors. Apart from this, wear out effects due to prolonged usage like Hot Carrier Injection (HCI) and Negative Bias Temperature Instability (NBTI) also degrade the performance of the devices. Unlike a PRNG, which relies on the algorithm to generate randomness, a TRNG depends on the performance and reliability of its circuit to generate un-bias and un-correlated output. Hence, it is essential to study the effect of operating conditions on the entropy of the TRNG output.

3.1 Effect of temperature on MOS transistor

The drain current of an NMOS transistor is given by the following equation [16].

$$I_{ds} = \begin{cases} 0 \quad for\ V_{gs} < V_t \\ \beta\left(V_{gs} - V_t - {V_{ds}}/{2}\right)V_{ds} \ for\ V_{ds} < V_{dsat} \\ \frac{\beta}{2}\left(V_{gs} - V_t\right)^2 \ for\ V_{ds} < V_{dsat} \end{cases} \qquad (3.1)$$

$$\text{where } \beta = \frac{(\mu_n * C_{ox} * W)}{L}$$

Hence, the drain current is a function of the electron mobility and the threshold voltage. Both these parameters are functions of the operating temperature. The mobility of electrons is given by:

$$\mu(T) = \mu(T_r)\left(\frac{T}{T_r}\right)^{-k} \qquad (3.2)$$

$$where, T = absolute\ temperature$$

$$T_r = room\ temperature$$

$$k = fitting\ parameter\ (in\ the\ range\ 1.2 - 2.0)$$

With an increase in temperature the mobility of electrons decreases. This would lead to a decrease in the drain current. But, the drain current is also dependent on the threshold voltage that is give by the equation

$$\boldsymbol{Vt(T) = Vt(T_r) - k(T - T_r)} \qquad (\mathbf{3.3})$$

$$where\ T = absolute\ temperature$$

$$T_r = room\ temperature$$

$$k = fitting\ parameter\ (in\ the\ range\ 0.5 - 3.0\ mV/K)$$

Hence with increase in temperature, the threshold voltage of the transistor decreases aiding the performance. But, it is observed that the net effect of increase in temperature is that the transistor drain current decreases and hence the delay of the transistor increases.

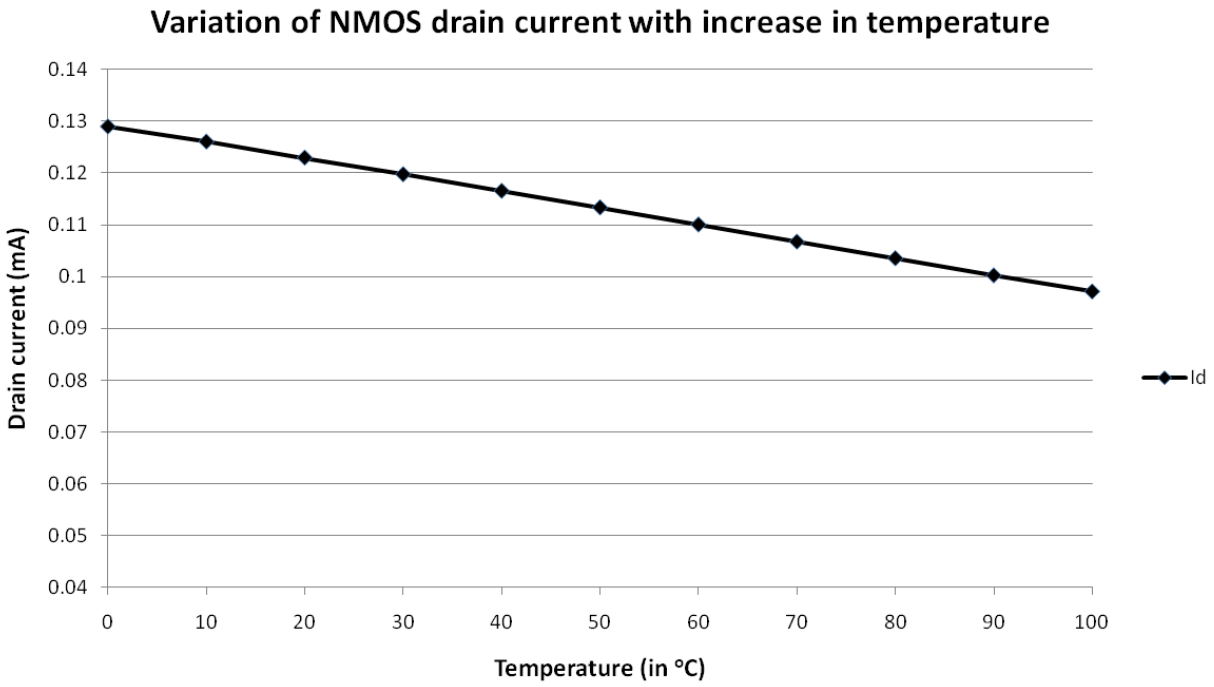


Figure 16. Variation of NMOS drain current with temperature

3.2 Effect of temperature on MOS transistor in the presence of process variation

For the study of Metastability based TRNG, the relative mismatch in the transistor parameters of the two cross coupled inverters is more significant than the absolute process variation. On similar lines, the relative effect of operating conditions on the transistors is of greater concern than the absolute effect. Thus, it is important to analyze the effect of variation of temperature for transistors with different channel lengths. The BSIM4 model indicates that as channel length decreases, the threshold voltage shows a greater dependence on the channel length due to Short Channel Effect (SCE) and Drain Induced Barrier Lowering (DIBL). The change in V_{th} due to SCE and DIBL is modeled as [17]

$$\Delta \boldsymbol{V_{th}} = -\boldsymbol{\theta_{th}}\left(\boldsymbol{L_{eff}}\right)[\mathbf{2}(\boldsymbol{V_{bi}} - \emptyset_{\boldsymbol{s}}) + \boldsymbol{V_{ds}}] \qquad (\mathbf{3.4})$$

$$where, \theta_{th}\left(L_{eff}\right) = short - channel\ effect\ coefficient$$

$$V_{bi} = built - in\ voltage\ of\ source\ or\ drain\ junction$$

The short-channel effect coefficient has a strong dependence on the channel length given by

$$\boldsymbol{\theta_{th}}\left(\boldsymbol{L_{eff}}\right) = \frac{\mathbf{0.5}}{\mathbf{cosh}\left(\frac{\boldsymbol{L_{eff}}}{\boldsymbol{l_t}}\right) - \mathbf{1}} \qquad (\mathbf{3.5})$$

$$where, l_t = characterisitc\ length$$

The temperature dependence of threshold voltage is given by the equation

$$\boldsymbol{V_{th}}(\boldsymbol{T}) = \boldsymbol{V_{th}}(\boldsymbol{TNOM}) + \left[\boldsymbol{KT1} + \frac{\boldsymbol{KT1L}}{\boldsymbol{L_{eff}}} + \boldsymbol{KT2}.\boldsymbol{V_{bseff}}\right]\left[\frac{\boldsymbol{T}}{\boldsymbol{TNOM}} - \mathbf{1}\right] \qquad (\mathbf{3.6})$$

$$where\ TNOM = Nominal\ temperature$$

$$KT1L = Channel\ length\ dependence\ of\ temperature\ coefficient\ for\ threshold\ voltage$$

Hence, with decreasing channel length, the short-channel effect coefficient increases. Thus, the change in V_{th} is larger. So, the net effect of decreasing mobility and decreasing threshold voltage will vary for transistors of different channel lengths. Transistors with shorter channel length may be expected to have a smaller reduction in drain current with increasing temperature because of a larger decrease in the threshold voltage.

Simulations were performed for varying transistor lengths and operating temperature by modeling in HSPICE. The drain current measured in each scenario is normalized against the drain current at 0^{o}C, which as expected is the largest.

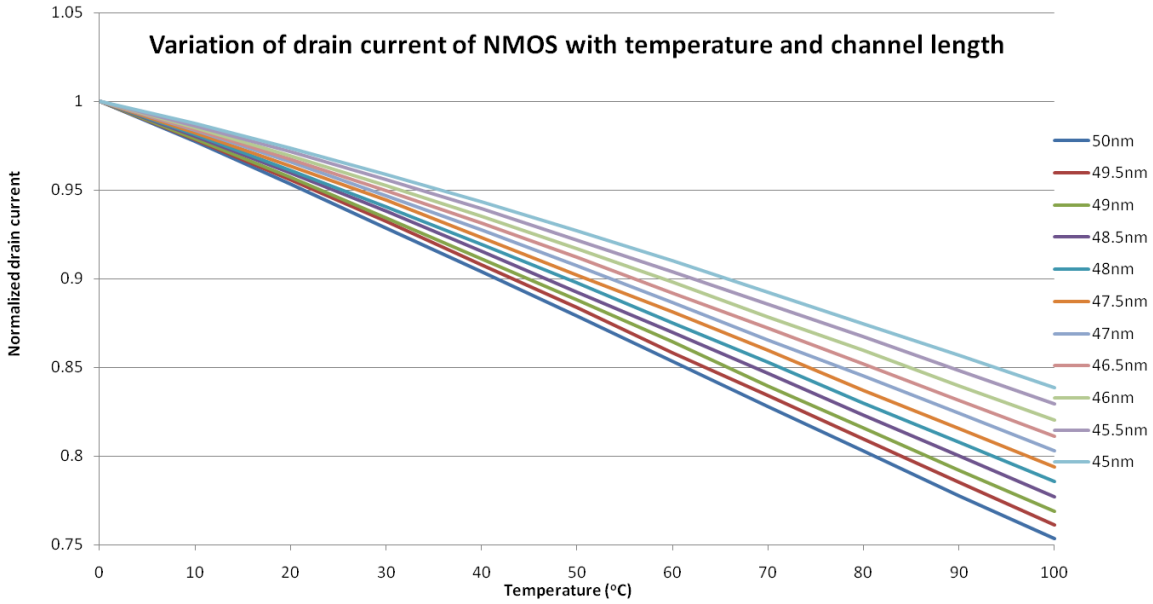


Figure 17. Variation of drain current of NMOS of different channel length with increase in temperature

The results, as shown in figure 17, indicate that transistors with longer channel length have a steeper slope of drain current reduction. This result reinforces the analytical reasoning provided earlier based on BSIM model equations. Hence, with decreasing channel length, the rate of decrease of drain current, with increase in temperature, is slower. Thus, for two transistors with

mismatch in device lengths, the relative difference between the transistor delays can be expected to increase with increase in temperature.

3.3 Effect of temperature on TRNG

The plots of drain current of two NMOS transistors with different mismatches at varying temperature are shown in figure 18. It is evident that, with greater mismatch, the difference in drain currents of the two transistors increases at a greater rate with increase in temperature.

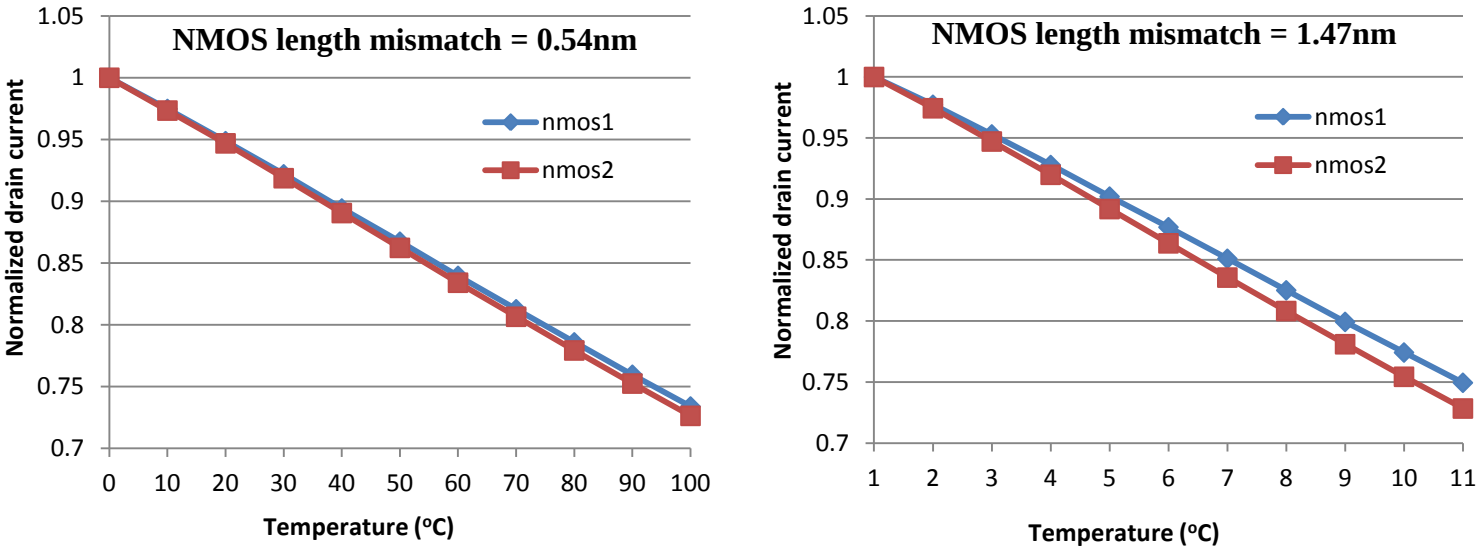
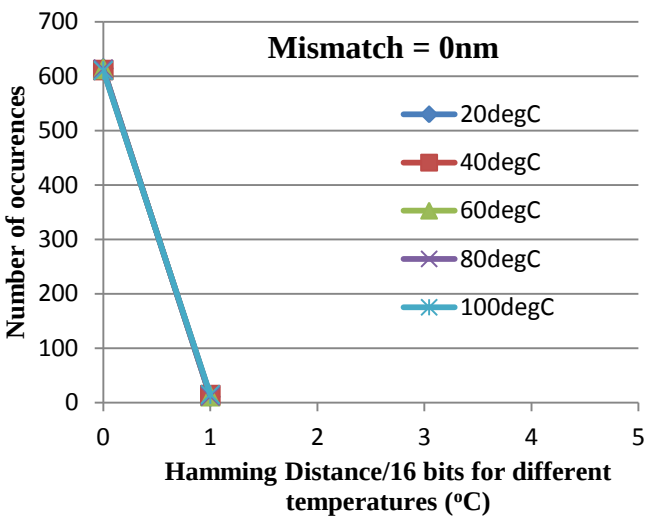


Figure 18: Rate of decrease in drain current for different values of device mismatch

To study the effect of temperature on the TRNG in the presence of process variation, the TRNG modeled in SPICE was simulated for varying temperature values and random variation in transistor lengths. Hamming distance between bits generated at different temperature corners is an effective metric used to analyze the effect of temperature. The results below represent the hamming distance of sequences of 16bits generated at different temperatures as compared to the bits generated at 0^{o}C.



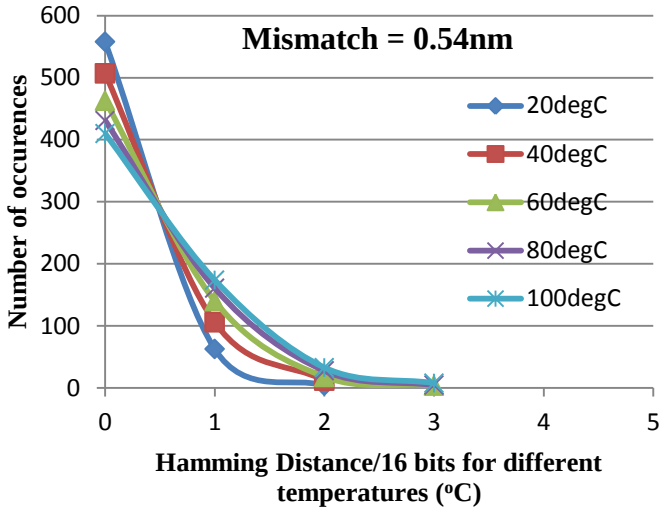
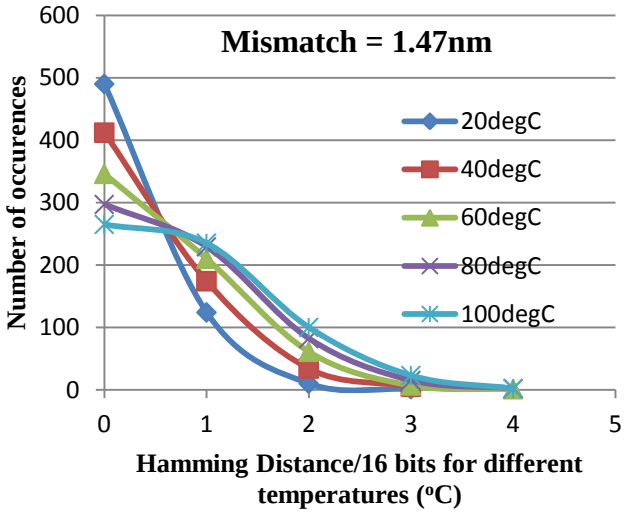


Figure 19: Hamming distance compared with TRNG at 0°C



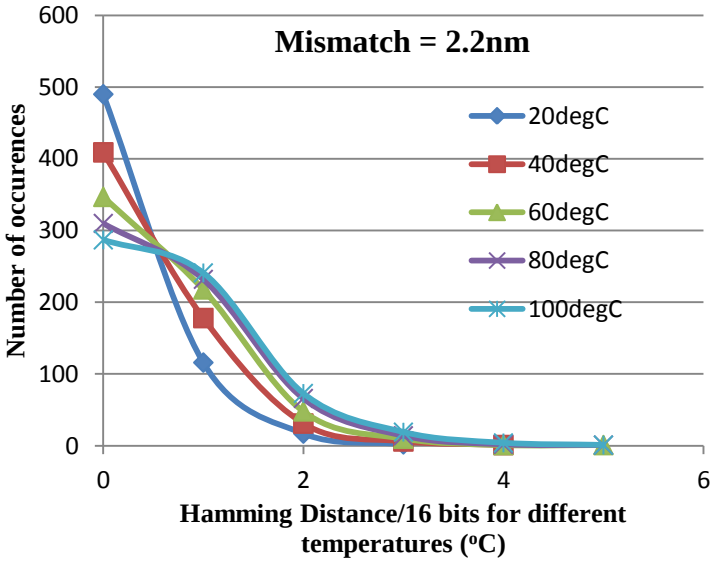


Figure 20: Hamming distance compared with TRNG at 0°C

The variation in hamming distance indicates that the statistics of the TRNG change with change in temperature. This directly translates into a change in the bit entropy. With increasing temperature, the bit entropy of the TRNG decreases. But, designs with greater mismatch are observed to have a steeper reduction in bit entropy. Hence, temperature has a greater impact on TRNG with larger device mismatch.

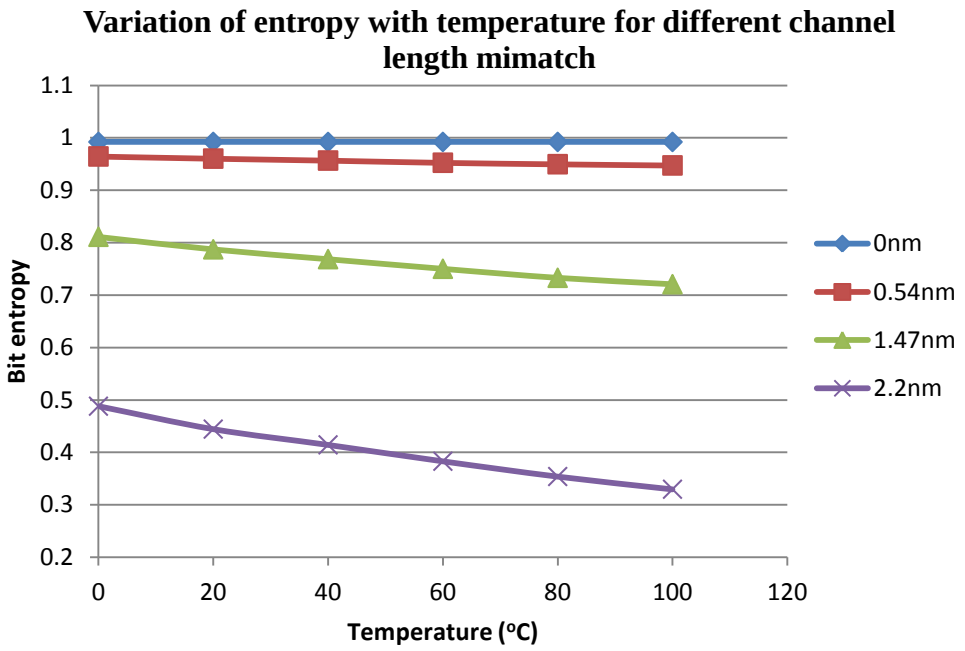


Figure 21: Variation of entropy with increase in temperature

3.4 Effect of power supply noise on the behavior of the TRNG

Similar to temperature, noise on the power supply can also affect the performance and behavior of circuits. In specific, for high performance designs, power supply noise can impact the delay of the cells and cause timing failures. Since metastability based TRNG is highly sensitive to difference in delay of the transistors, it is important to analyze the behavior of the TRNG in the presence of power supply noise.

To study the effect of supply noise, the TRNG was simulated for random device mismatches and a power supply noise of 5% of VDD at 200MHz. Hamming distance for sequences of 16 bits was calculated comparing with a TRNG with stable power supply. The results indicate that power supply noise does not have a significant impact on the statistics of the TRNG. While designs with minimal device mismatch are robust against supply noise and designs with large device mismatches are already too biased to see any effect of power supply noise. A slight variation in the bit distribution is observed in designs which have mismatch ranging from 2-6%.

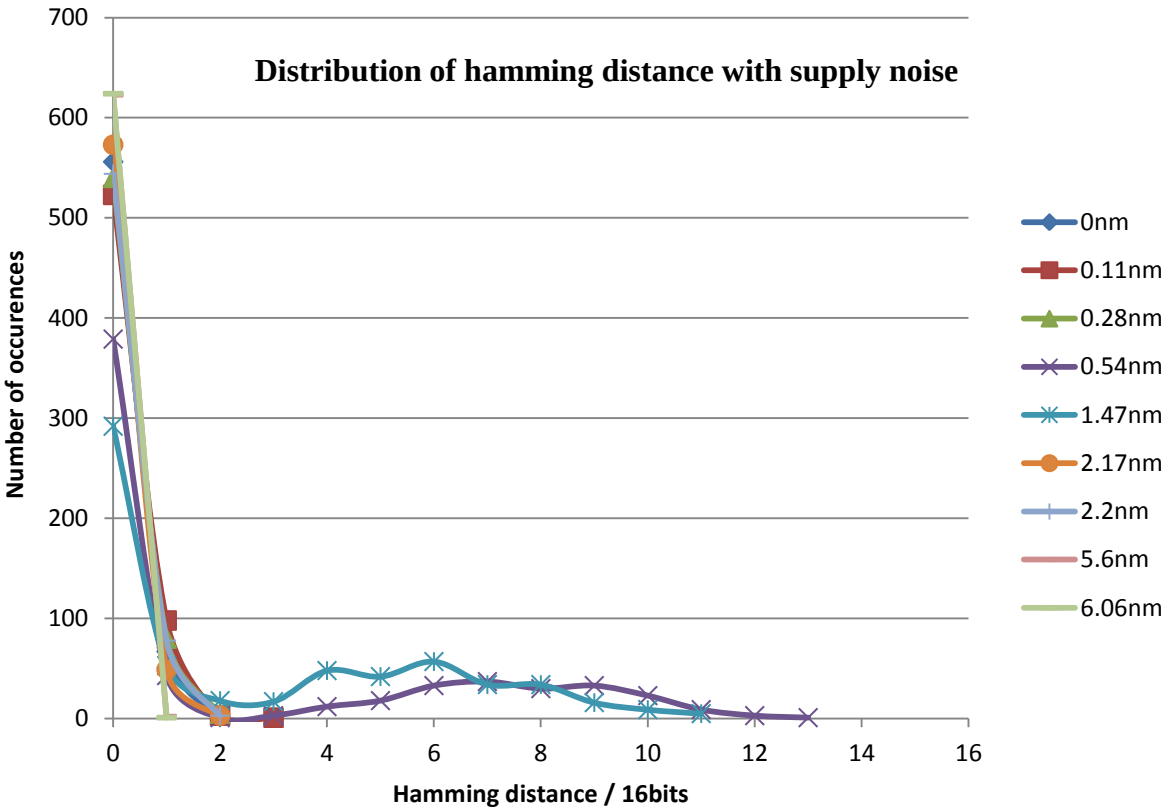


Figure 22: Hamming distance of bits compared with TRNG with stable power supply

The effect of supply noise on the entropy is negligibly small and has no noticeable trend across varied device mismatches.

As discussed in the previous chapter, circuit calibration techniques can be employed to mitigate the effect of process variation. But, a one-time tuning at the testing stage does not resolve the problem of effect of temperature on the design. Any calibration performed at the testing stage can only account for the process variation at the testing temperature. Any variation in temperature during the chip operation will again bias the TRNG.

Hence, a dynamic self-calibration mechanism has to be used to mitigate the effect of temperature variation. The TRNG circuit also needs to be analyzed for the effect of fluctuations in supply voltage and the impact of wear out effects like HCI and NBTI/PBTI.

CHAPTER 4

SUB-VDD PRECHARGE TECHNIQUE

One of the ways to improve the randomness of the TRNG and the effectiveness of post-processing techniques is to make the TRNG circuit inherently more stable against device mismatch. 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. Here we explore a sub-vdd precharge technique to reduce the effect of intra-die variation on the entropy of the TRNG.

4.1 Effect of pre-charge on TRNG bias

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],

$$\boldsymbol{I_{dsat} = \frac{\mu_0 C_{ox} W}{2L} \left(V_{gs} - V_t\right)^2} \qquad (\mathbf{4.1})$$

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

$$\boldsymbol{I_{dsat} = \frac{\beta W}{L} \left(V_{gs} + V_{noise} - V_t\right)^2} \qquad (\mathbf{4.2})$$

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,

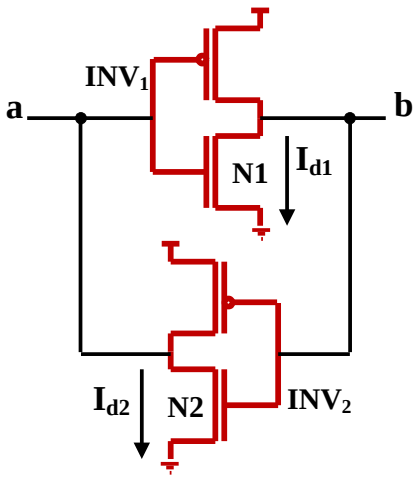


Figure 23: Cross-coupled inverters

$$I_{dsat1} = \frac{\beta W_1}{L_1}\left(V_{gs} + V_{noise1} - V_{t1}\right)^2 \qquad (4.3)$$

$$I_{dsat2} = \frac{\beta W_2}{L_2}\left(V_{gs} + V_{noise2} - V_{t2}\right)^2 \qquad (4.4)$$

Under ideal conditions, when the NMOS devices are perfectly matched, Idsat1 = Idsat2 for Vnoise1 = Vnoise2. In other words, the state of the TRNG is resolved based only on the differential thermal noise Δnoise = Vnoise1 - Vnoise2 . 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,

$$I_{dsat1} - I_{dsat2} > 0, for\ V_{noise1} = V_{noise2} \qquad (4.5)$$

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 Vt, the difference in the NMOS currents is given by,

$$I_{dsat1} - I_{dsat2} = \left(\frac{\beta W_1}{L_1} - \frac{\beta W_2}{L_2}\right)\left(V_{gs} + V_{noise} - V_t\right)^2 \quad (4.6)$$

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, Vnoise is a random variable and cannot be controlled, for a given device type (Typical/High/Low Vt), the effect of device mismatch can be reduced by lowering the Vgs. 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],

$$\Delta V_{th}(SCE, DIBL) = -\theta_{th}(L_{eff})[2\,(V_{bi} - \phi_s) + V_{ds}] \quad (4.7)$$

where, ΔVth is the change in threshold due to Short Channel Effect (SCE) or Drain Induced Barrier Lowering (DIBL); θth(Leff) is the short channel effect coefficient; Vbi is the built-in junction voltage; and Vds 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,

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

$$I_{dsat1} - I_{dsat2} = \left(\frac{\beta W}{L}\right)\left[\left(2V_{gs} + 2\,V_{noise} - V_{t1} - V_{t2}\right)\left(V_{t2} - V_{t1}\right)\right] \quad (4.8)$$

Equation (9) also shows that a reduced Vgs 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 indicates 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.

4.2 Effect of process variation on TRNG offset voltage

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 N1 is faster than N2, then I1 > I2 for V(a) = V(b). But, for a large enough $\Delta V=V(b)-V(a)$, I1 = I2. This is the differential voltage required to negate the mismatch and equalize the pull down currents. From the transistor current equation (6), it is 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.

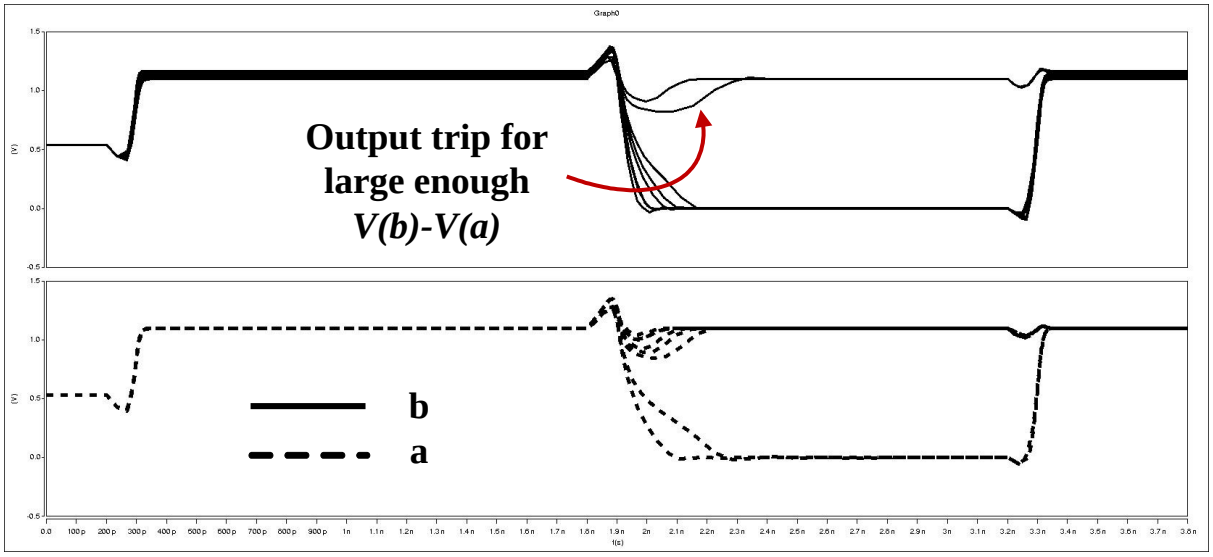


Figure 24: Effect of increasing differential voltage on biased TRNG

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 Vgs 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.

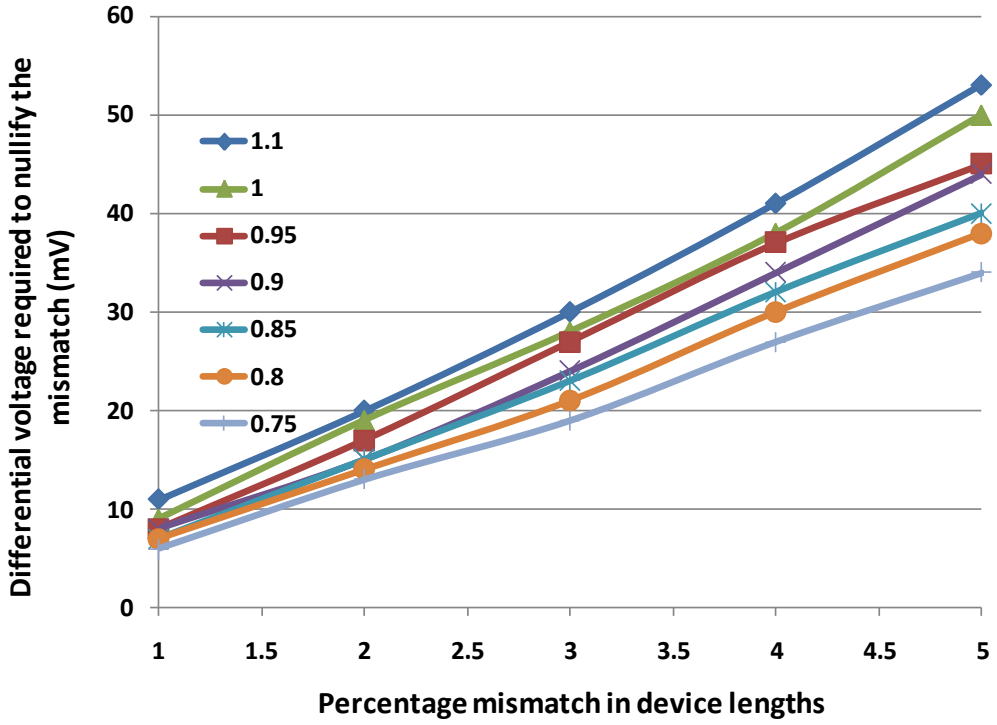


Figure 25: Analysis of differential voltage to compensate mismatch

For 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 $\Delta V=V(b)-V(a)$ 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, figure 26. 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.

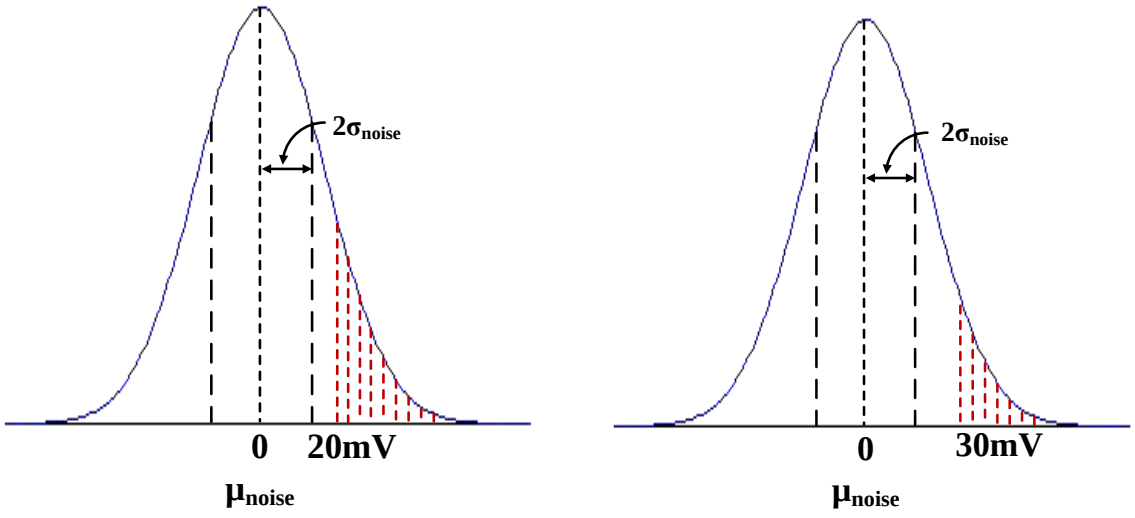


Figure 26: Distribution of thermal noise

4.3 Implementation and results with sub-vdd pre-charge

The pre-charge circuit is designed using pull down load on the pre-charge paths as shown in figure 27. 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. Figure 28 shows the voltage drop obtained due to NMOS and PMOS pull down devices of different sizes.

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. Figure 29 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.

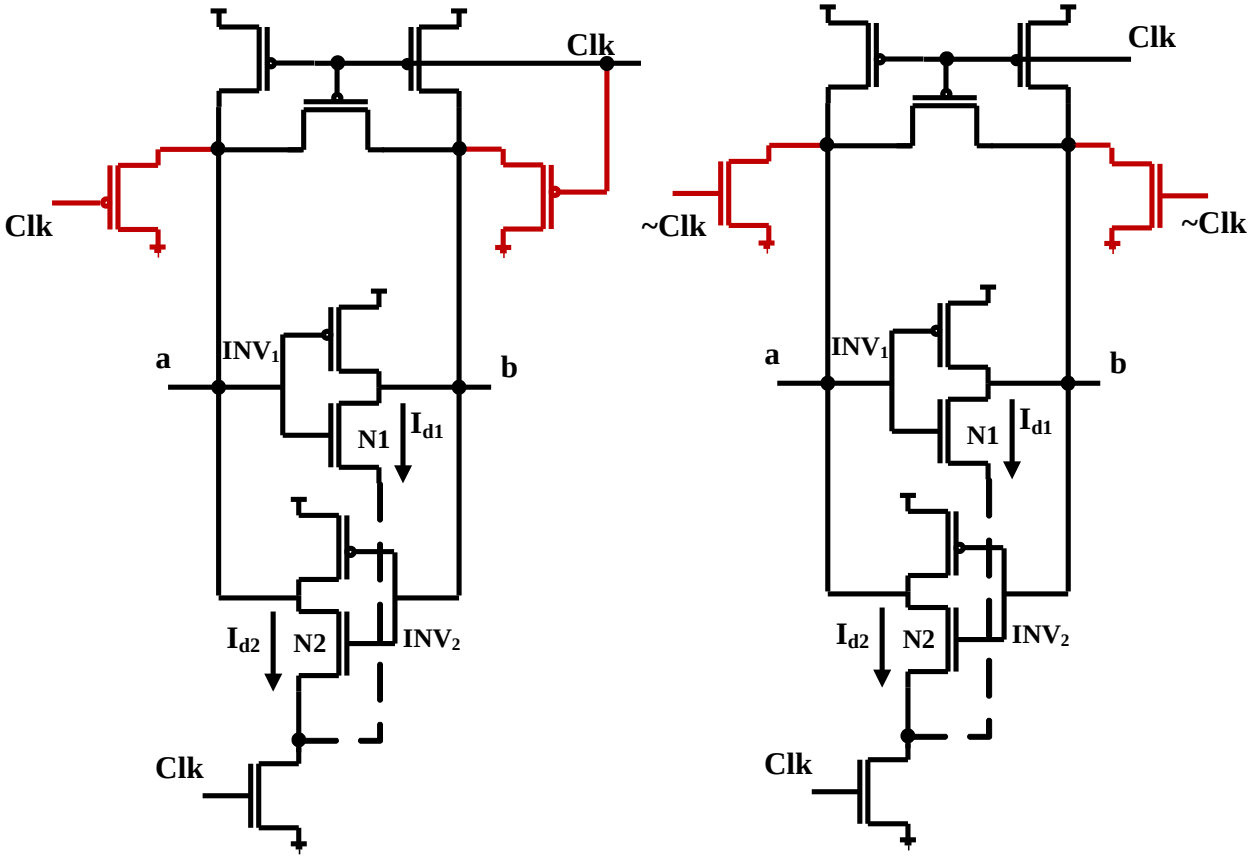


Figure 27: Circuit to generate sub-vdd pre-charge voltage

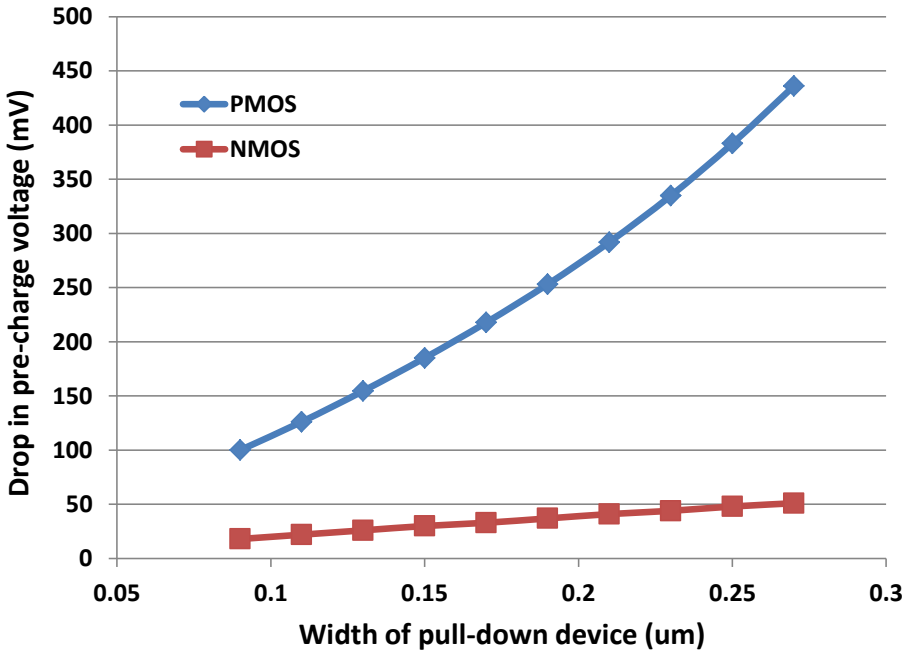


Figure 28: Effect of NMOS and PMOS load on pre-charge nodes

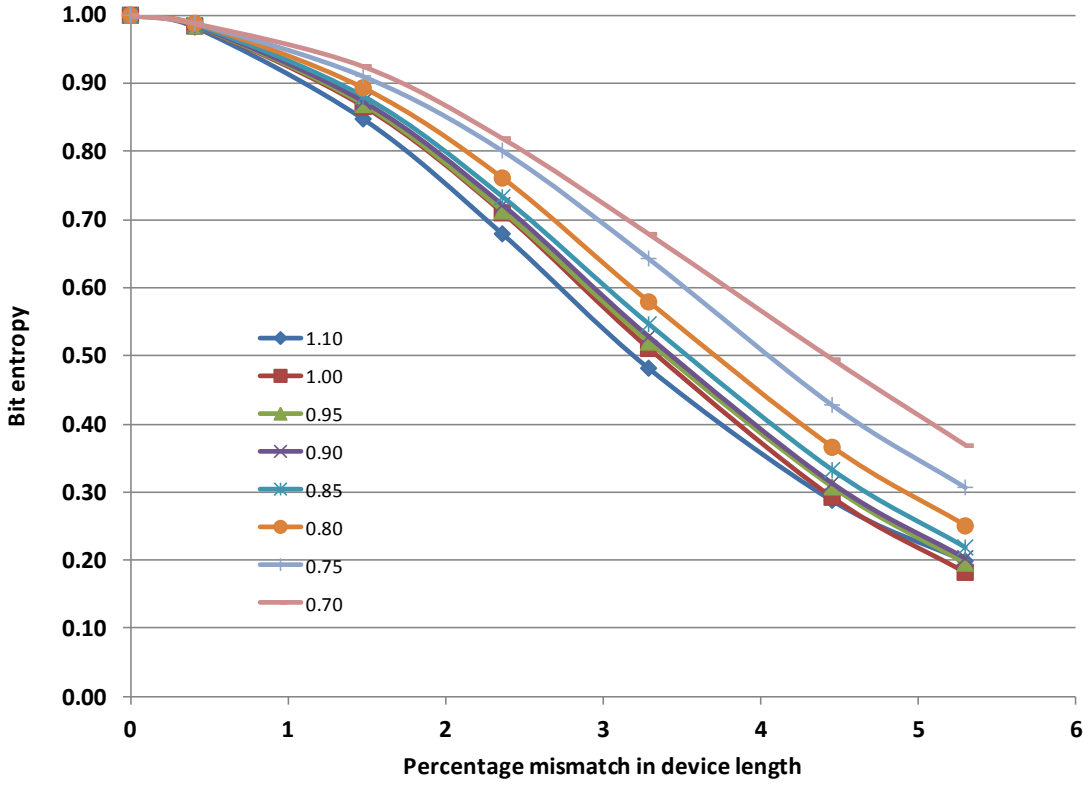


Figure 29: Bit entropy with increasing device mismatch and varying pre-charge voltage

Thus, using a sub-vdd pre-charge voltage makes the TRNG more robust to process variation. However, the sub-vdd pre-charge technique by itself cannot enhance the entropy of the TRNG by enough to be used for cryptographic applications. But, a TRNG with inherently better bit entropy feeding a post-processing unit can be expected to be more robust that a TRNG with traditional Vdd pre-charge. Further, this technique only reduces the pre-charge time, but has no impact on the evaluation time of the TRNG, which limits the TRNG circuit performance.

CHAPTER 5

HYBRID SELF-CALIBRATION TECHNIQUE FOR ENTROPY EXTRACTION

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 [23]. 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 [24][25]. S. Bijansky *et al.* have proposed the use of variable supply voltages to improve parametric yield of designs in [26]. 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 [27]. The variable delay tuning techniques may be implemented both in the form of tuning at the testing phase or online automatic/adaptive tuning [28]. 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 [29]. B. Dutta *et al.*[30] 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.

Circuit calibration is a very effective technique to mitigate the effect of process variation. But, calibration performed during chip testing has some disadvantages. Chip testing is one of the most expensive steps in the VLSI design and fabrication process. The time duration of testing

governs the chip testing cost. Hence, calibrating the TRNG at the testing phase is not a cost effective solution for low cost designs like RFID. Calibration at the testing phase does not provide a dynamic extraction mechanism. As a result, any variation in the operating conditions cannot be compensated on the fly. Further, wear out effects like Hot Carrier Injection (HCI) and Negative/Positive Bias Temperature Instability (NBTI/PBTI) cannot be corrected. Hence, an efficient self-calibration mechanism has to be developed to ensure a cost effective and dynamic approach to entropy extraction.

In [18], Srinivasan *et. al* have proposed a self-calibration technique. The calibration circuit is similar to the one in [14] and consists of coarse and fine grain calibration steps. A state machine is implemented to continuously monitor the output of the TRNG. On power up, the coarse calibration is activated to account for the large mismatch in the cross-coupled inverter. Once two bit flips are observed at the output of the TRNG, the control enters into the fine-grain calibration. Here the delay on the pre-charge clock is continuously varied based on the output bit of the TRNG. The self-calibration technique incurs additional overhead in the implementation of the control logic. Further, the configuration process is performed every cycle of the TRNG operation. Hence, the configuration bits are switched every cycle. This leads an overhead in energy that may be expensive for applications like RFIDs and sensor nodes. Continuous calibration increases the correlation between bits generated since the bias is continuously modified based on the previous output. Although a bit-entropy ~1 is achieved, increased correlation will weaken the statistics of the TRNG.

To overcome these short comings, we propose a hybrid self-calibration technique that incorporates a combination of coarse level tuning using adaptive circuit calibration and a static entropy extraction using algorithmic techniques to compensate for finer mismatch.

5.1 Proposed hybrid self-calibration technique

The results from the initial study of comparison of various entropy extraction techniques are as shown in figure 30. The results indicate that algorithmic technique like XOR

function and von Neumann correction are efficient for device mismatches of upto 2%. These techniques incur lesser overhead in terms of energy and implementation. Further, they do not increase the correlation of the bits generated by the TRNG. Hence, we explore a hybrid self-calibration technique where the circuit is initially calibrated using additional transistors to overcome the coarse mismatch between the devices and operate the TRNG in a region equivalent to 2% device mismatch. Then, the adaptive coarse calibration is stopped and an algorithmic technique like XOR function or von Neumann corrector is used to provide continuous static entropy extraction.

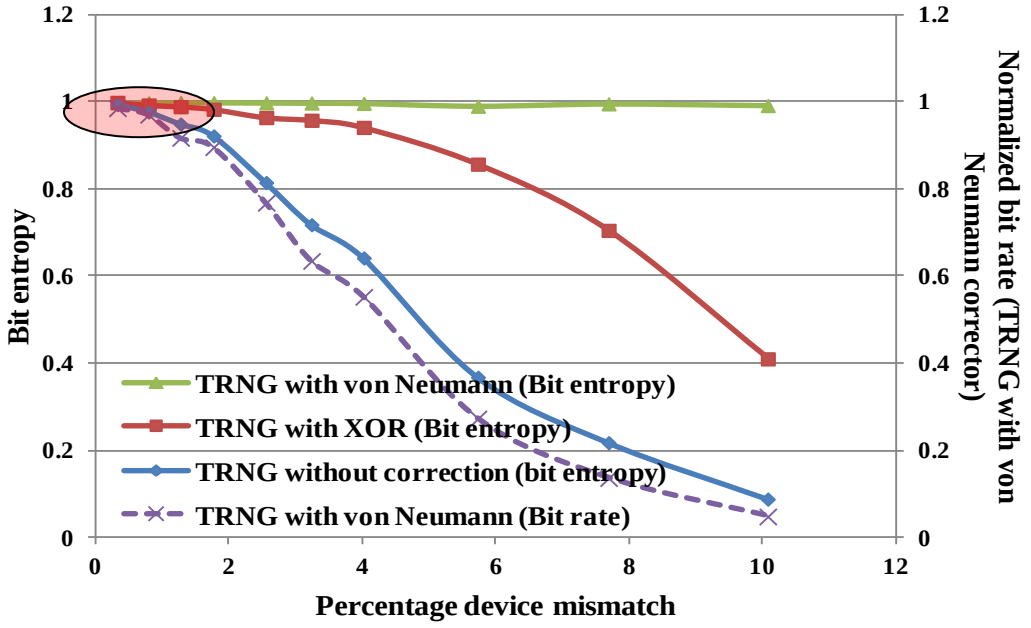


Figure 30: Effectiveness of algorithmic technique for smaller mismatch

The hybrid self-calibration technique is implemented as shown in figure 31. Since both the nodes “a” and “b” of the TRNG are pre-charged to Vdd each cycle, the mismatch in the pull down devices is seen to have a more significant impact than the mismatch in the pull up devices. Hence, we provide parallel NMOS devices which can be configured match the pull down current in the cross coupled inverters. The output of the TRNG is monitored by a control logic that configures the additional pull down transistors till output of the TRNG flips twice. At this stage

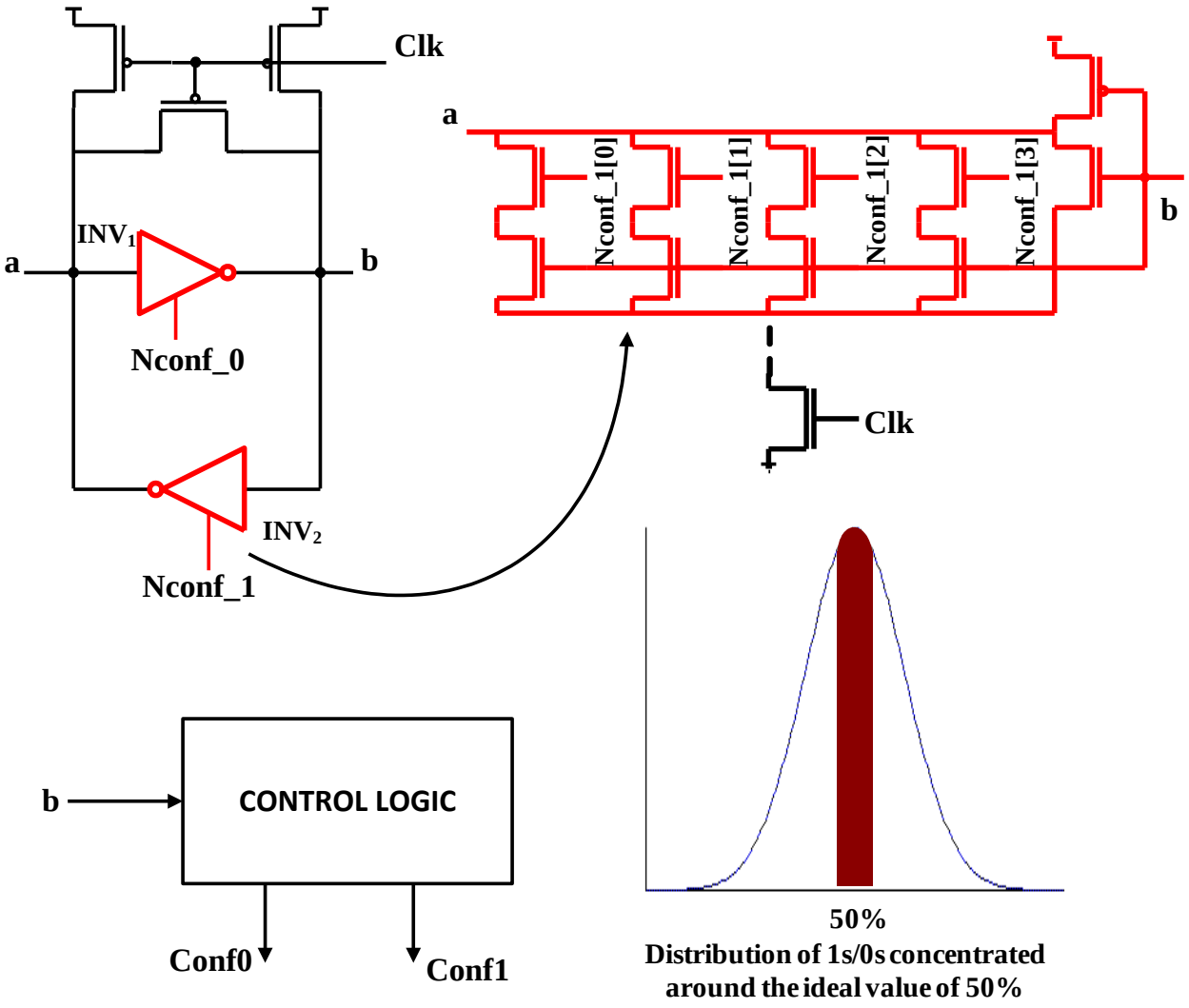


Figure 31: Coarse circuit self-calibration

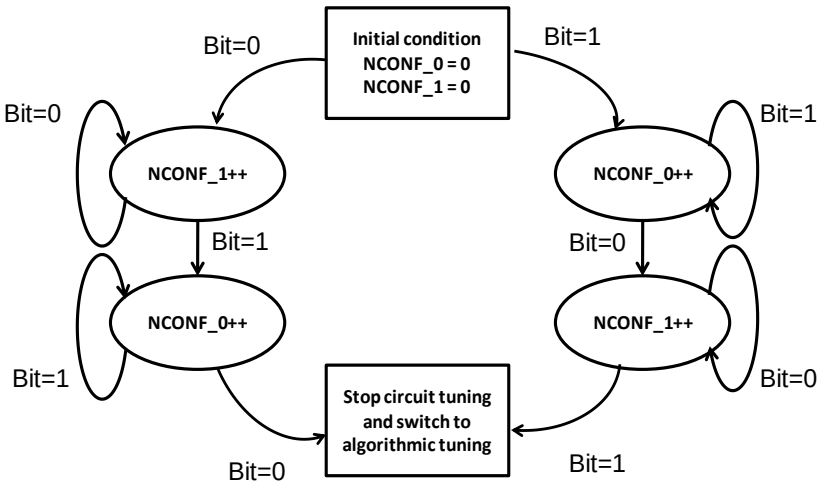


Figure 32: State machine for control of circuit calibration

the TRNG is compensated for large variations and the bit distribution enters the highlighted region, close to the ideal value of 50%. The control logic stops the coarse calibration.

The calibrated TRNG can be fed to an entropy extractor using XOR function or von Neumann corrector. The XOR function and von Neumann correctors provide near ideal entropy if the TRNG circuit feeding them is calibrated to operate in a region close to the ideal scenario.

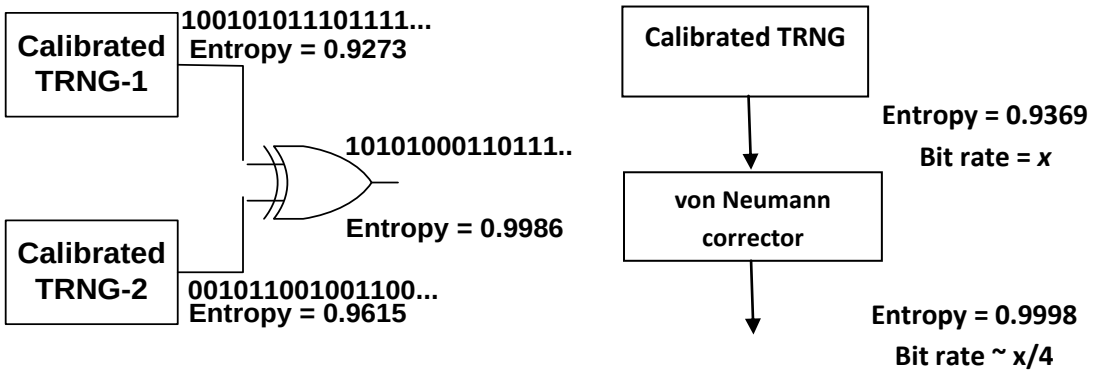


Figure 33: Algorithmic post-processing for finer entropy extraction

5.2 Implementation 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

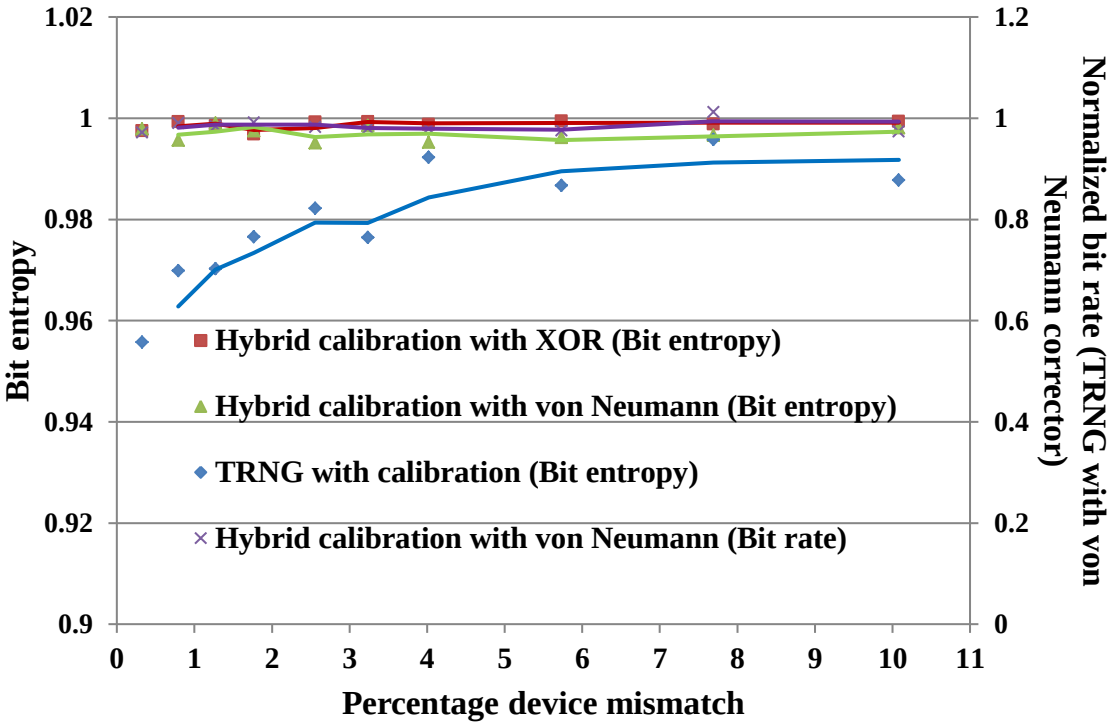


Figure 34: Entropy extraction with hybrid self-calibration

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.

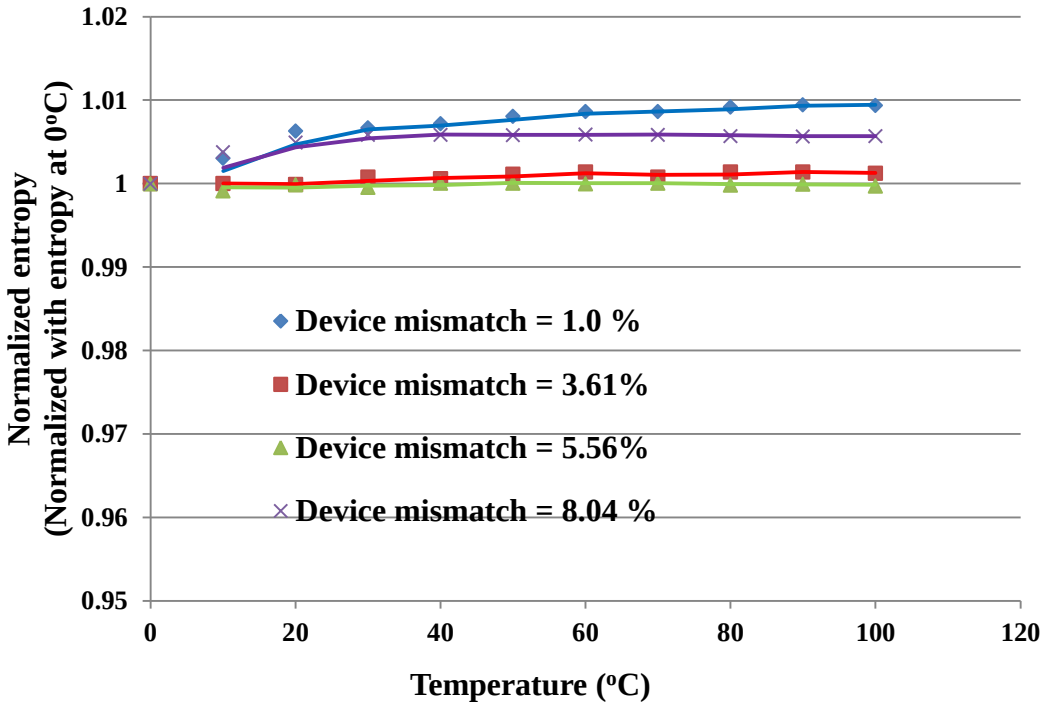


Figure 35: Robustness of hybrid self-calibration against variation in temperature

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.

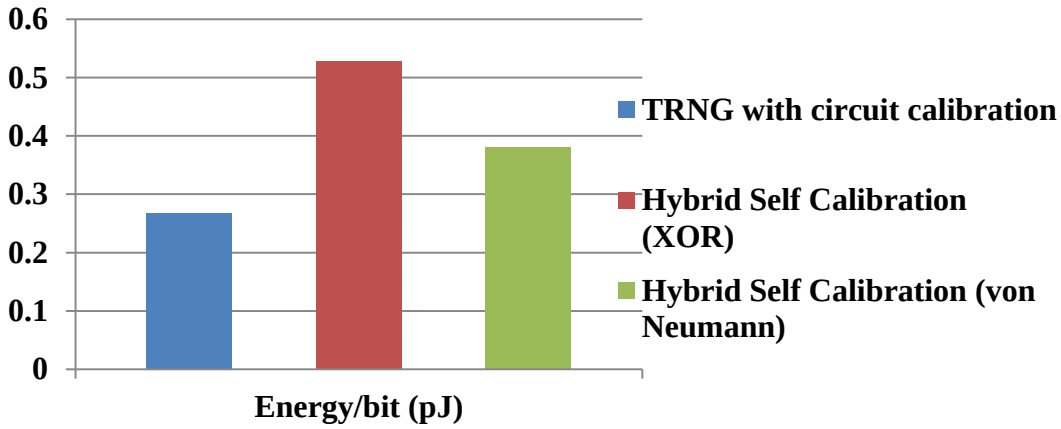


Figure 36: Energy overhead with hybrid self-calibration (pre-charge = 1.1V)

5.3 Hybrid self-calibration with sub-vdd pre-charge

Although lower pre-charge voltage, described in the previous chapter, 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 results indicate that using a lower pre-charge further enhances the effectiveness of hybrid self-calibration technique. This is due to the fact that the underlying TRNG circuit operation is more robust and hence the self-calibration technique provides a much better improvement in entropy as compared to the traditional pre-charge technique.

The results as shown in figure 37 for self-calibration using XOR function and figure 38 for self-calibration using von Neumann function further establish that pre-charging the TRNG to a lower voltage improves the entropy.

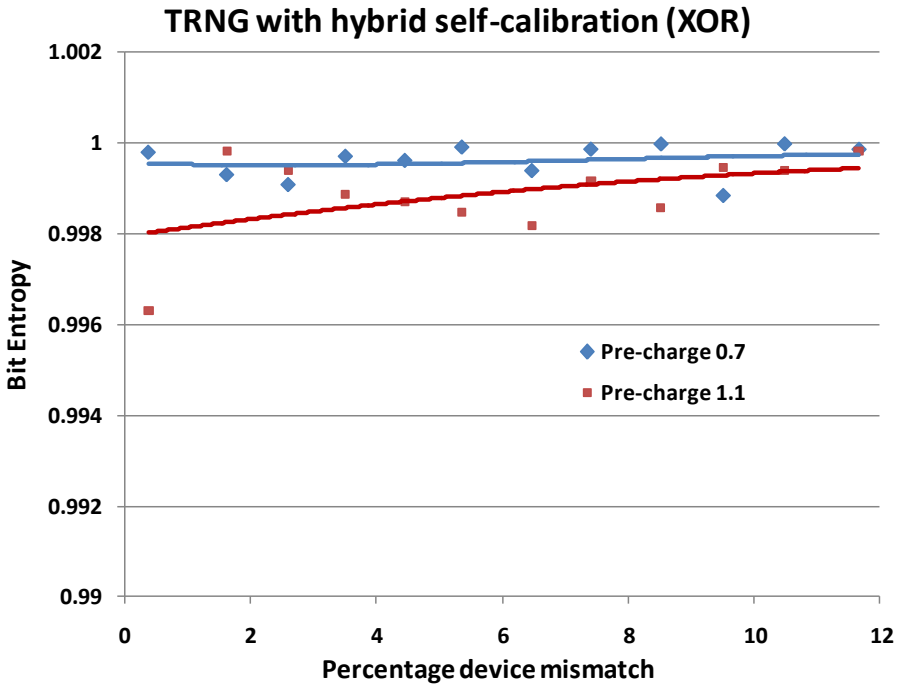


Figure 37: Comparison of hybrid self-calibration with different pre-charge voltages (XOR function)

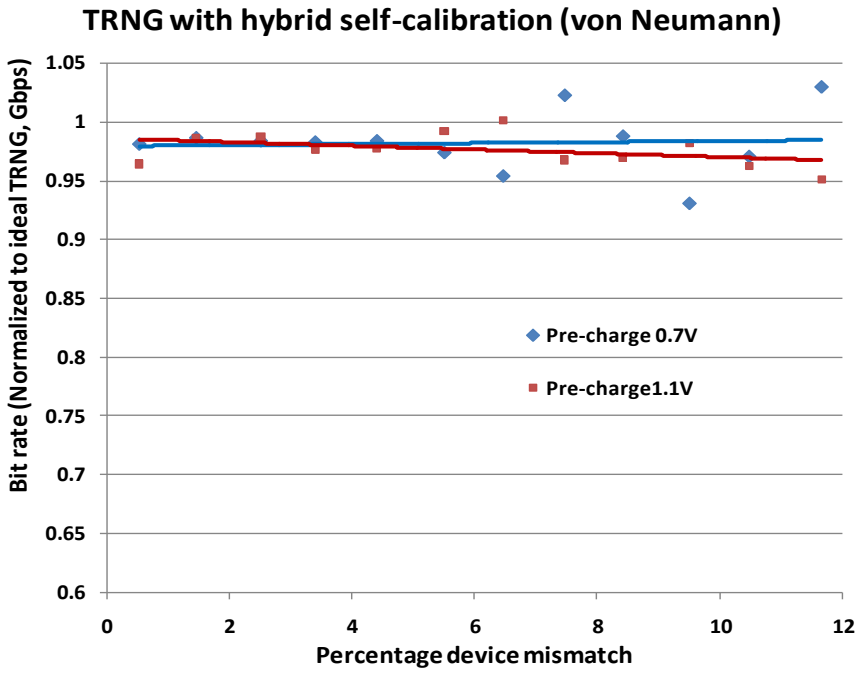


Figure 38: Comparison of hybrid self-calibration with different pre-charge voltages (von Neumann function)

In this chapter we propose a hybrid self-calibration technique that utilizes circuit calibration to correct coarse mismatches in the cross-coupled inverters to operate the TRNG in a near ideal scenario. Then, algorithmic technique is used to further correct the mismatch and extract entropy without introducing any correlation in the bits. The control logic used for coarse calibration is active only during the power up of the TRNG and hence contributes only to leakage power in the long run. The hybrid self-calibration is further incorporated with sub-vdd pre-charge technique to further enhance the randomness of the TRNG output.

CHAPTER 6

ATTACK MODELS FOR TRNG

Study of attack models forms a very crucial area in the field of security. For a cryptographic system extracting keys or id from a TRNG, the TRNG could potential be a single point of attack to weaken the entire system. Hence, it is important to analyze the possible vulnerabilities of TRNG and design techniques to mitigate the same.

Traditional PRNG have been broken and various algorithms for the same have been published [19][32]. A PRNG can be subjected to non-invasive attacks, where the attacker monitors the output of the PRNG and tries to determine the sequences that may be generated by cryptanalysis of the observed data. This is possible since a PRNG is algorithm based and consecutive states or bits of a PRNG are not completely independent. A weak LFSR may be broken by a sheer brute force attack using the immense computational resources available today. PRNG may also be subjected to the modern forms of attacks based on Differential Power Analysis (DPA) or Electro-Magnetic emissions (EM). Apart from the simple LFSR based PRNG design, a number of secure PRNG algorithms are used in real-world crypto systems. Some of these are ANSI X9.17 PRNG, the DSA PRNG, the RSAREF PRNG and CryptoLib. These algorithms have also been demonstrated to be vulnerable to cryptanalytic attacks. In [32], a study of cryptanalytic attacks on these real-world PRNG has been demonstrated. The PRNG circuits may be subjected more complex attacks like a) Direct Cryptanalytic Attack, b) Input-Based Attacks and c) State Compromise Extension Attacks. These attacks are limited by the computational resources available to an attacker.

An ideal TRNG on the other hand cannot be attacked using a non-invasive method since it is unbiased and there exists no correlation between the bits generated. Any form of brute force technique becomes near impossible for large key lengths of the order of 128 bits. But, the efficiency of a TRNG circuit depends on factors like fabrication process and operating conditions. Variation in these factors, either naturally or as introduced by an attacker can degrade

the performance of the TRNG from a cryptographic sense. So, these factors provide avenue for an attacker to either utilize the existing imperfection in the design or introduce the same to reduce the randomness of the bits generated. Attacks have been demonstrated using simple non-invasive technique like frequency injection can make the RO based TRNG on real EMV card deterministic [20]. The different factors that may have implications on the attack of a TRNG are discussed below.

6.1 Process variation

Variation in the fabrication process is one of the major factors affecting the performance of the TRNG. Mismatch in the parameters of the transistors in the form of channel length or width and differences in threshold voltage (V_{th}) bias the TRNG to generate bits of one polarity with a greater probability than the other. If this variation is uncompensated, the key or id space of the TRNG bits generated is reduced. This would help an attacker to model the output of the TRNG based on the probability of the bits generated.

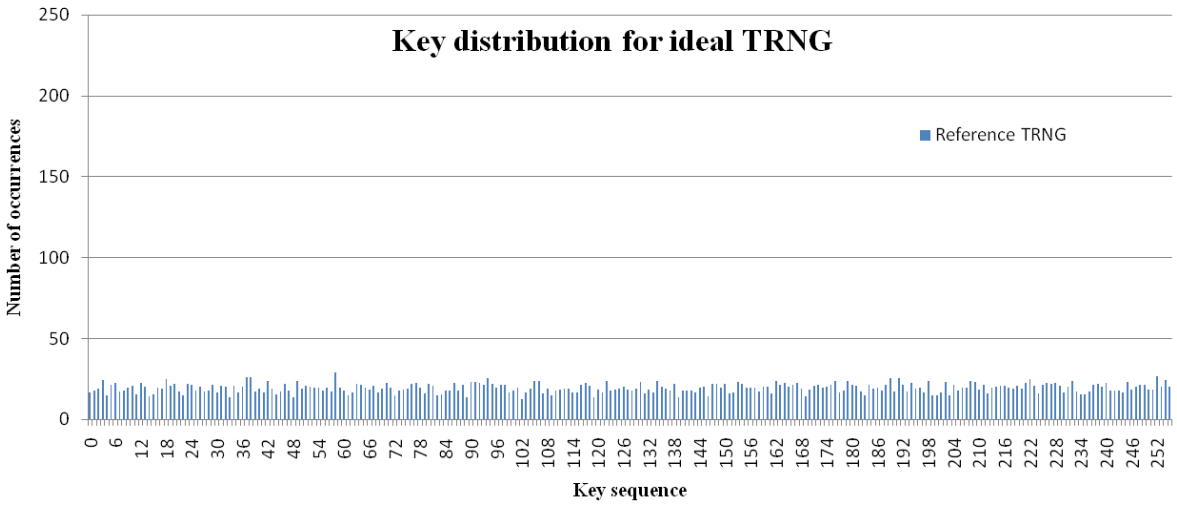


Figure 39. Distribution of 8-bit key for ideal TRNG

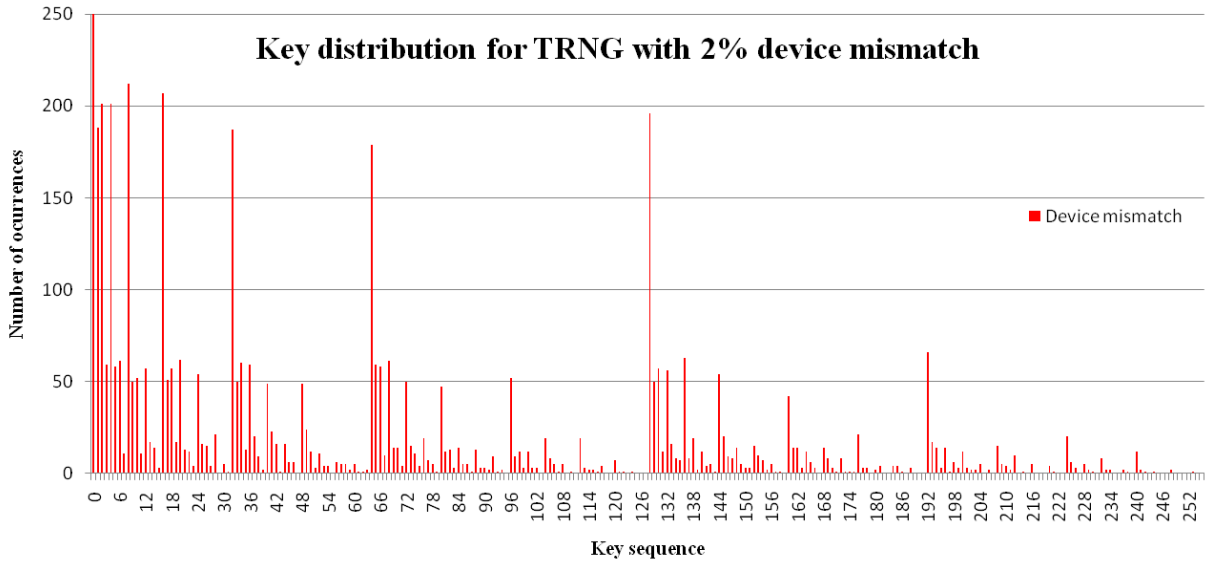


Figure 40. Distribution of 8-bit key for TRNG with 2% device mismatch

The plots show that in the presence of process variation, the probability of occurrence of some 8-bit key sequence is significantly more that of others. Although an attacker might have no control over this factor in most cases, there are possibilities of tampering the circuit at the fabrication stage. Even a minute mismatch in the structure of the transistors in the inverters could reduce the entropy of the bits generated by a large number.

6.2 Operating temperature

Temperature affects the delay of transistors by changing in charge mobility and threshold voltage. The effect of temperature is observed to be different for transistors of different channel lengths. This effect can be utilized by an attacker to increase bias in a TRNG. Any post-processing technique can only increase the entropy of a TRNG. It may not be possible to converge on the ideal value of '1'. Thus, by increasing the temperature, an attacker can increase the difference in the delays of the inverters and hence increase the bias. The temperature may be increased through external sources or by activating on-chip circuits like a ring oscillator.

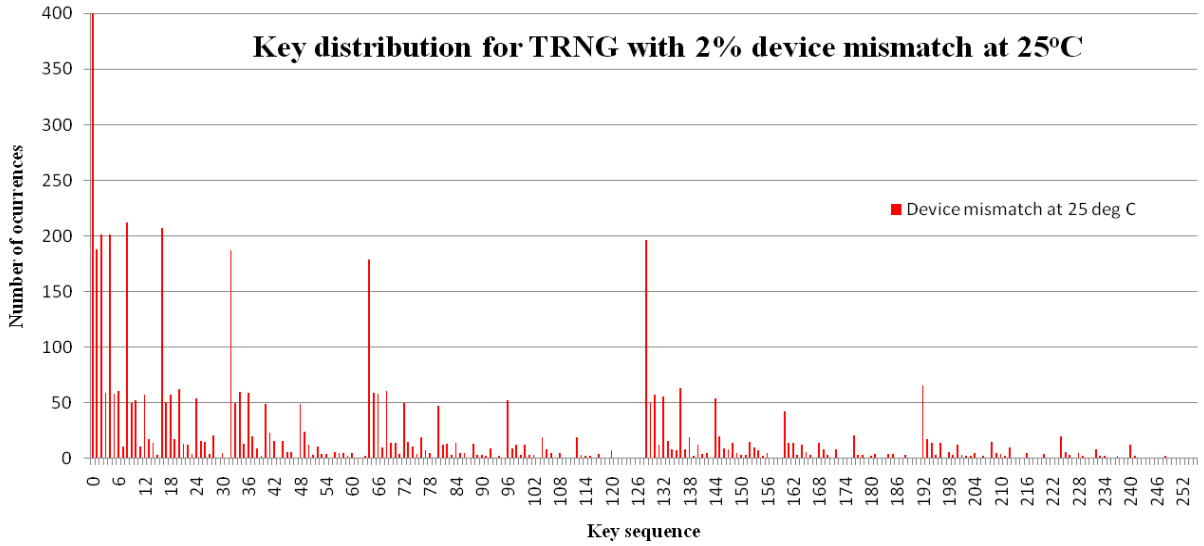


Figure 41. Distribution of 8-bit key for TRNG with 2% device mismatch operating at 25°C

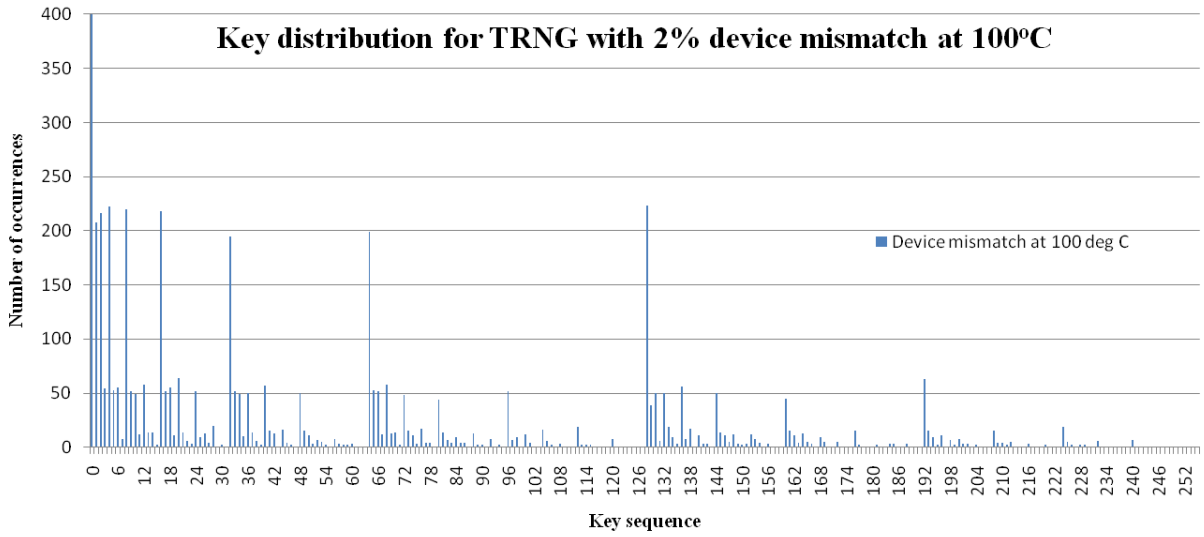


Figure 42. Distribution of 8-bit key for TRNG with 2% device mismatch operating at 100°C

The key distribution plots for 25°C and 100°C for a TRNG with 2% device mismatch show that with increase in temperature, the uniformity in distribution of random bit sequences decrease. As a result, it becomes easier for an attacker to model the TRNG and predict its outputs. A more evident metric is the byte entropy of 128-bit keys generated from the output of the TRNG at the two temperatures. The table clearly indicates a loss in byte entropy as temperature is increased.

Table 4. variation of byte entropy with increase in temperature

	TRNG with 2% mismatch at 25°C	TRNG with 2% mismatch at 100°C
Byte entropy for 8-bits	6.0326	5.6640
Byte entropy for 128-bits	96.5223	90.6254

6.3 Varying Supply voltage

The TRNG circuit involves some delay for both nodes to be pre-charged once a bit is generated. Similarly, there is a delay involved in resolving to stable state once the cross-coupled inverter enters a meta-stable state. This evaluation time is dependent on the differential thermal noise at the two nodes of the TRNG. Larger the differential, smaller will be the evaluation time. A plot of variation of evaluation time with varying differential noise is as shown in figure 43.

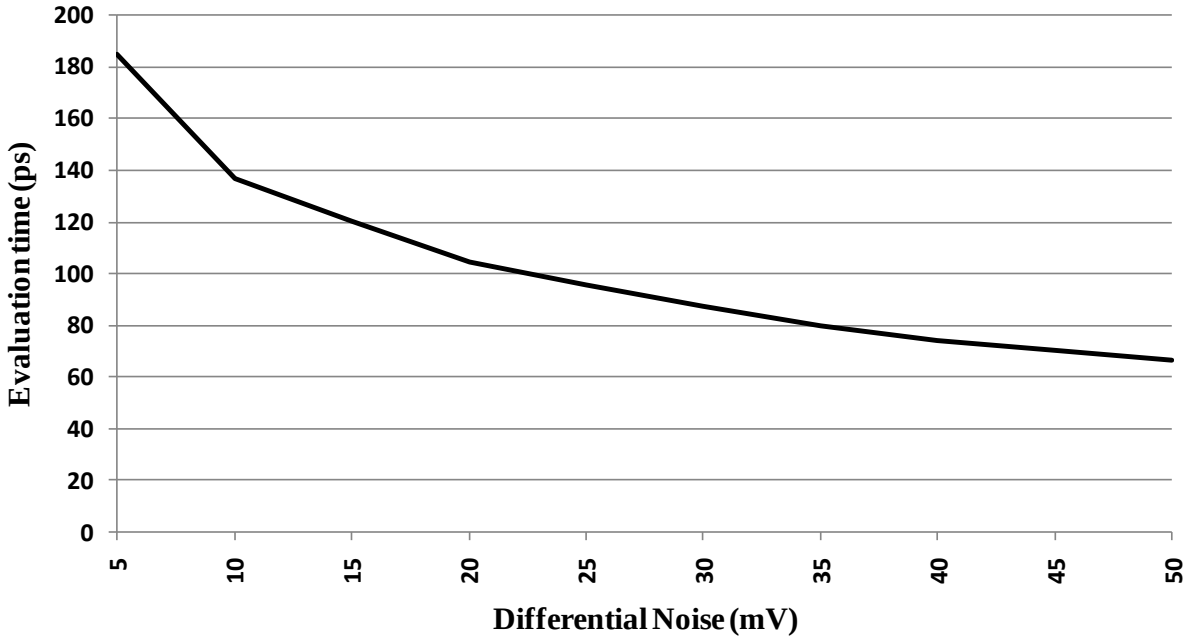


Figure 43: Variation of evaluation time with differential noise

The evaluation time is also a function of the supply voltage since a lower supply voltage increases the delay of the cross-coupled inverters to stabilize. In other words, the gain of the cross-coupled inverter decreases with decreasing operating voltage. Figure 44 shows the variation of pre-charge and evaluation time with variation in supply voltage. As the supply voltage is decreased, there is a small increase observed in the pre-charge time. But, the increase in evaluation time with decrease in supply voltage is significant.

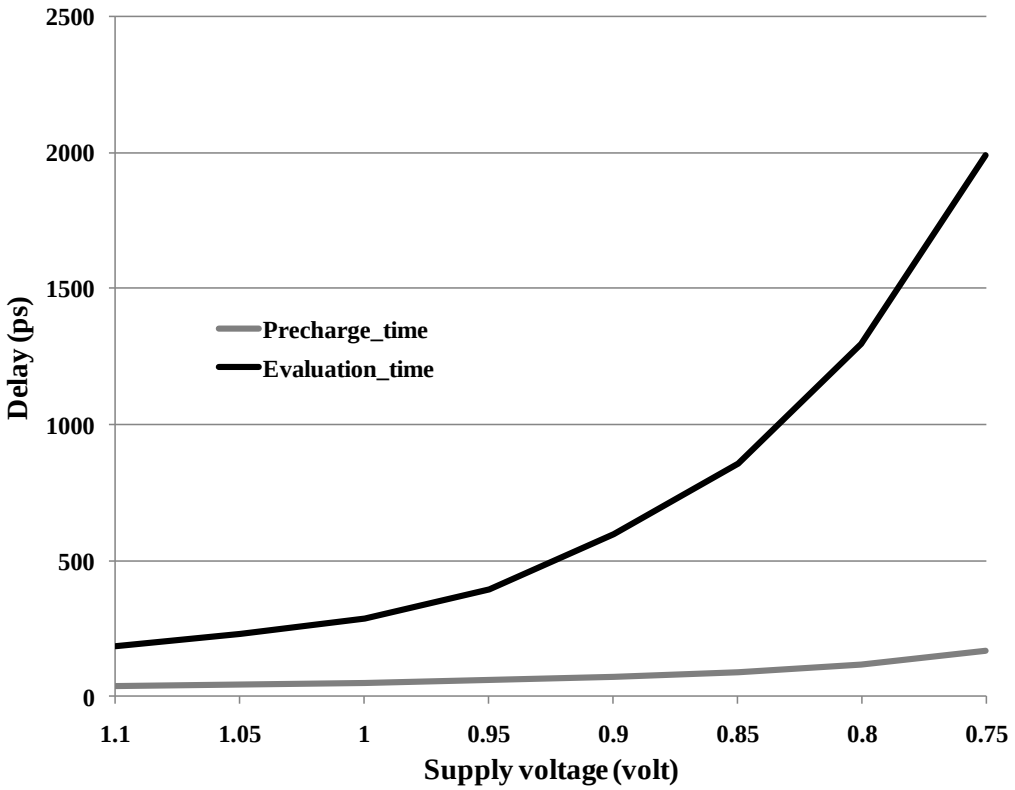


Figure 44: Variation of pre-charge and evaluation time with supply voltage

The above observation indicates that the performance of the TRNG can be controlled by an attacker by controlling the power supply voltage. The device sizing in the TRNG circuit is performed in accordance with the target operating frequency or the bit rate. The pre-charge and evaluation part of the clock cycle are just enough to meet the delay of the circuit. By decreasing the voltage an attacker can increase the evaluation time, keeping the clock rate constant. Figure 45 shows the variation of evaluation time with decreasing supply voltage.

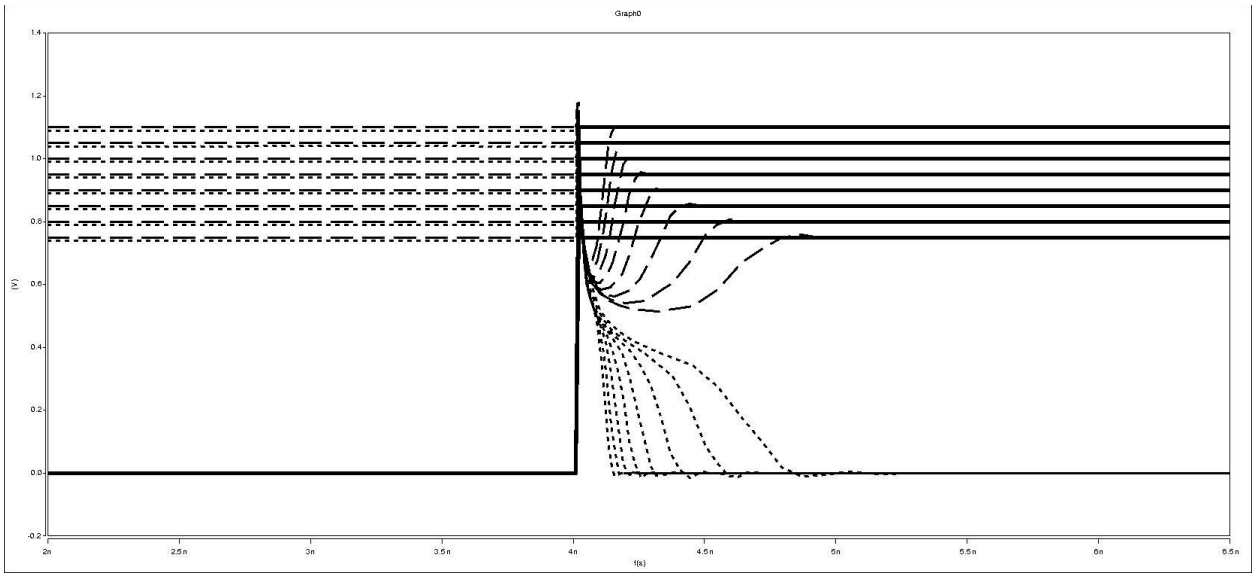


Figure 45: Variation of evaluation time with decreasing operating voltage

In a circuit optimized to operate at a specific frequency, by decreasing the power supply voltage, an attacker can cause incorrect bit read at the output of the TRNG. Figure 46 shows one of the output nodes of a TRNG designed to operate at 1GHz. With decreasing supply voltage, the evaluation time of the TRNG increases beyond a point where the pre-charge phase starts in between the evaluation. This causes the output of that node to be wrongly read as a one instead of a zero. Since the evaluation time of the TRNG is also a function of the differential noise, not all bits may be erroneous.

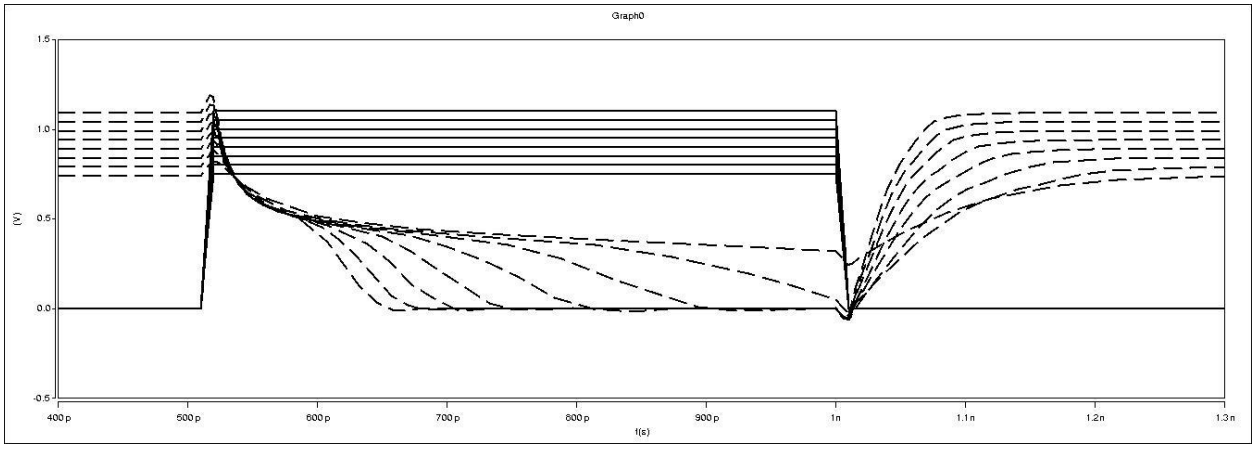


Figure 46: Erroneous bit due to reduced supply voltage

Figure 47 shows the variation in bit entropy for a TRNG under reduced supply voltage attack. It is seen that the bit entropy decreases rapidly as the supply voltage is reduced beyond 0.85V.

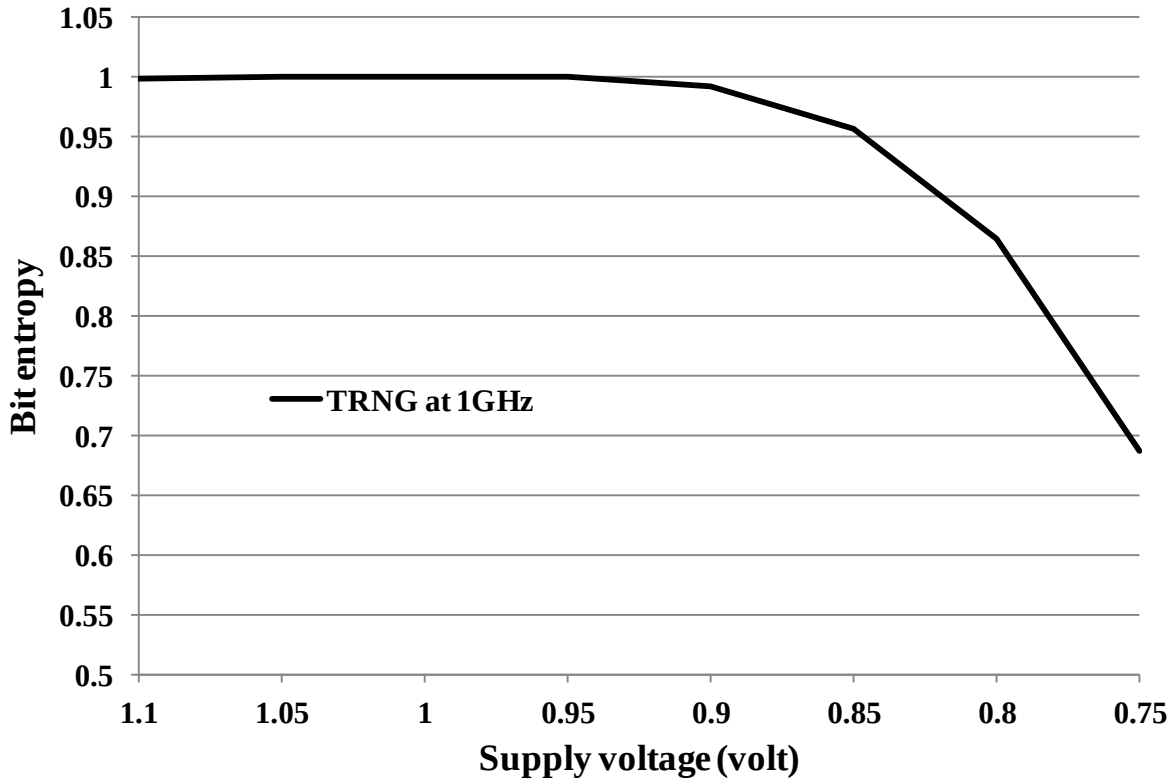


Figure 47: Variation of entropy with decreased power supply voltage

6.3.1 Detection of attack

An attack of the sort discussed above where the entropy of the TRNG is compromised by an active attack can be detected by feeding the output both of the nodes of the TRNG to an XOR/XNOR gate. It should be observed that according to the previous discussion, only a bit zero can be erroneously read as a bit one. But, in a TRNG the two nodes generate complementary bits. Hence, if one of the bits is driven to zero under a non-attack mode, the other node has to be driven to a stable state of one. Under an attack scenario, both nodes are seen to generate a bit "1" (or a bit "0" if the inverted outputs are read). Hence, by feeding both the nodes to an XOR/XNOR gate, an attack scenario can be detected.

6.3.2 Prevention of attack: asymmetric duty cycle

The results in figure 44 indicated that the pre-charge time of the TRNG is significantly lower than the evaluation time. Further, the pre-charge time is dependent only on the supply voltage. At 1.1V, the pre-charge time is 40ps. This value increases to 166ps for a supply voltage of 0.75V. Hence, a TRNG operating at 1GHz with a 50-50 ON-OFF duty cycle provides the entire negative half cycle of 500ps for the pre-charge phase. This provides enough margin for the pre-charge, some of which can be utilized for the evaluation phase to protect the TRNG from power supply reduction attack.

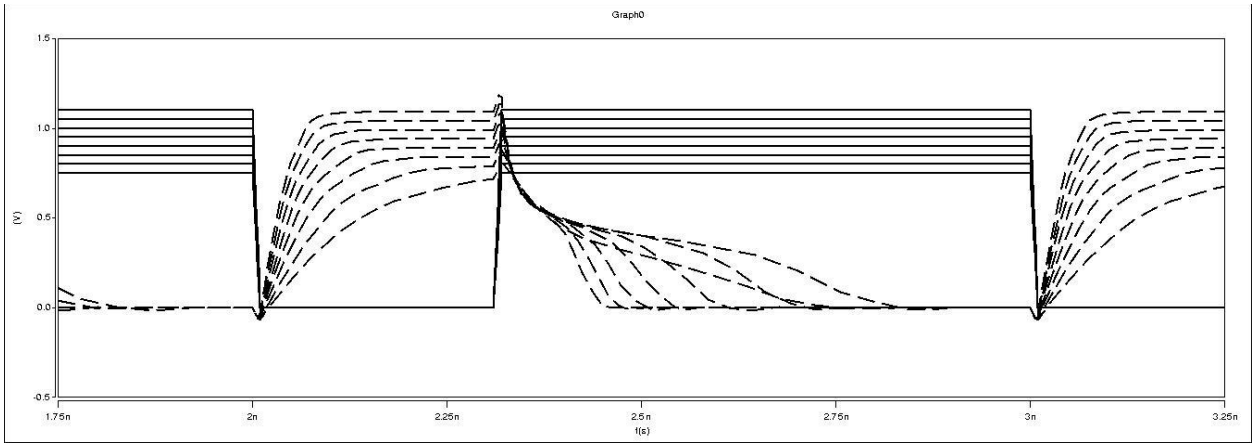


Figure 48: Voltage scaling attack prevention using asymmetric duty cycle clock

Figure 48 shows the effect of varying the duty cycle. The evaluation sequence is provided with more margin even if the supply voltage is reduced to 0.75V by keeping the clock signal high for 700ps in a 1ns clock. The variation in duty cycle is limited by the pre-charge delay. The effect of varying the duty cycle to protect the TRNG is shown in figure 49. For a 80-20 ON-OFF duty cycle, the TRNG is resistant to voltage scaling attack for upto 0.8V.

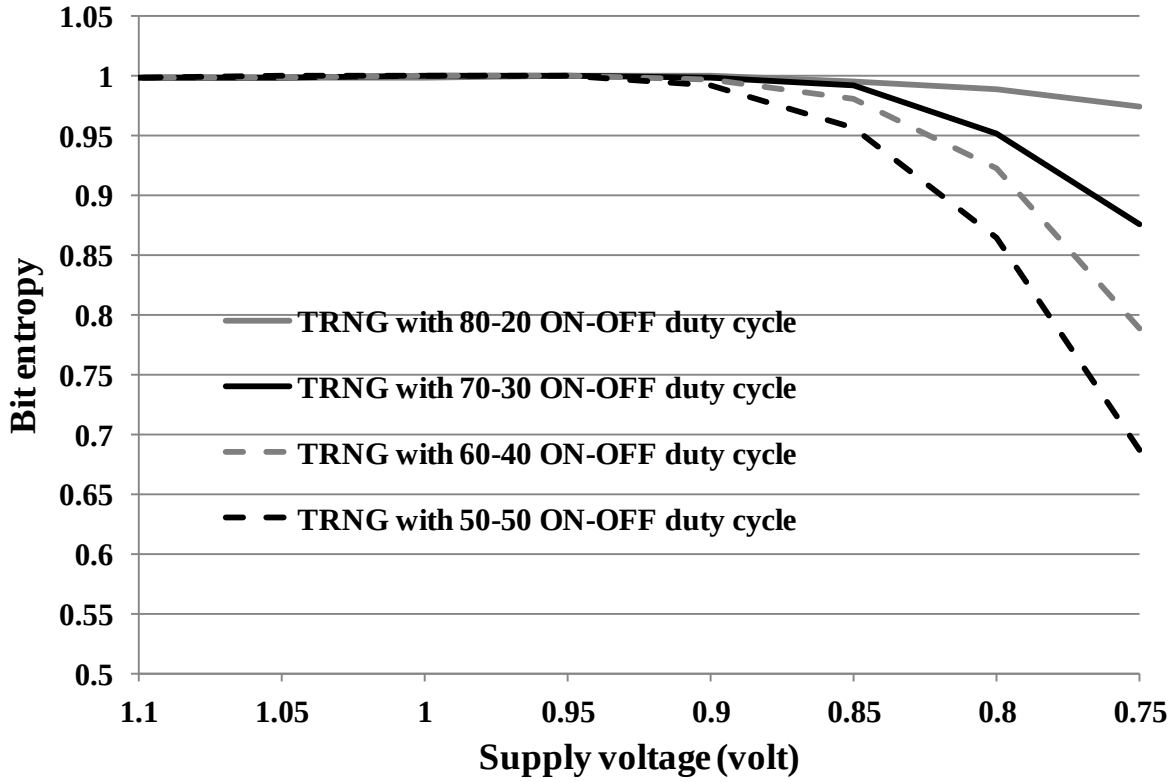


Figure 49: Bit entropy of TRNG with asymmetric duty cycle

6.4 Varying duty cycle of clock

Varying the duty cycle to favor the evaluation time was shown as one of the possible techniques to protect the TRNG against attacks. On similar lines, an attacker can control the clock signal to the TRNG to vary the duty cycle of the clock to decrease the evaluation period. In such a scenario, the TRNG may generate erroneous bits when the evaluation delay is close to the period of the positive cycle of clock. Figure 50 shows the impact of variation in duty cycle on the randomness of the output of the TRNG. Beyond a 35-65 ON-OFF duty cycle, the bit entropy decreases significantly. The TRNG can be protected against a varying duty cycle attack by providing enough margin using larger inverters or additional PMOS devices to increase the gain of the cross-coupled inverter.

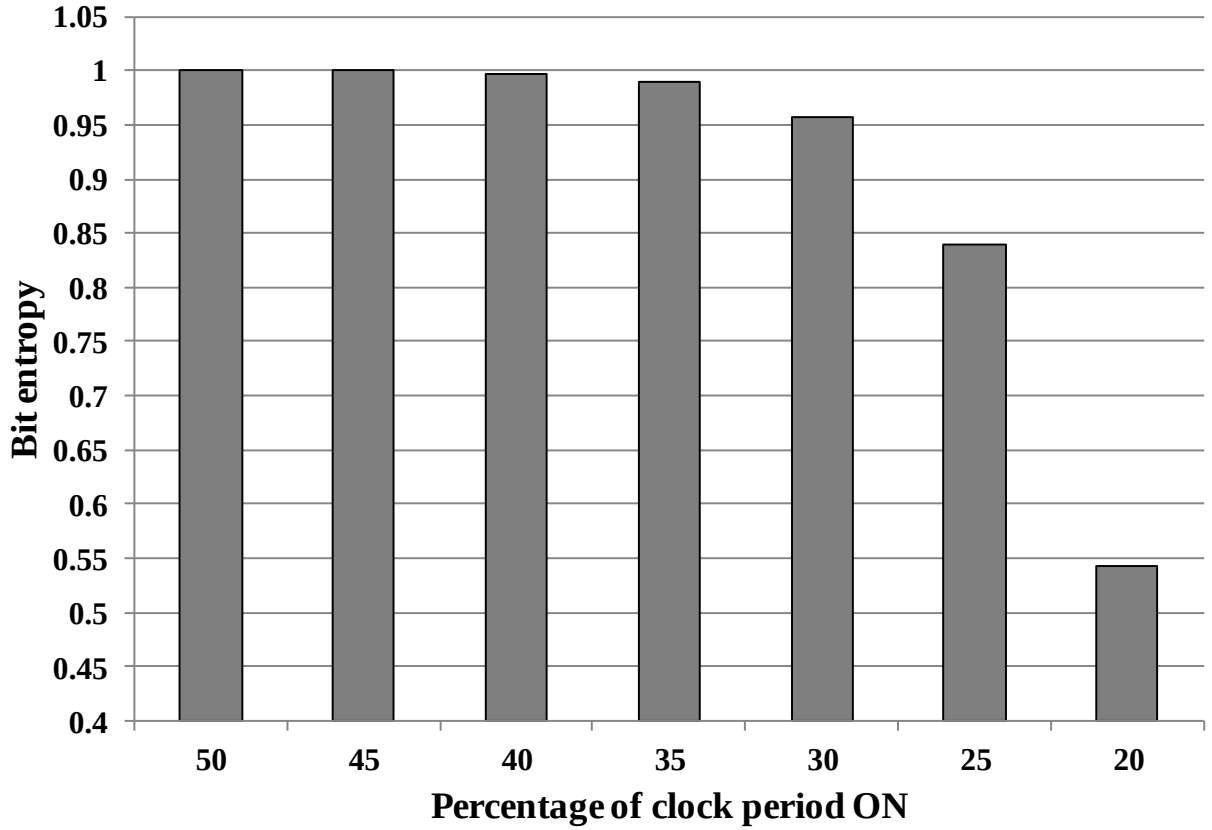


Figure 50: Attack on TRNG by varying clock duty cycle

6.5 Crosstalk

Designs are getting denser as more transistors are packed in smaller area. This has increased the number of interconnects in the design. Reduced spacing between interconnects and increasing height of the metal layers has increased the effect of cross talk. For a meta-stability based TRNG, that is highly sensitive to any mismatch, cross talk could act as a potential mode of attack. The Predictive Technology Models estimate a coupling capacitance 0.054fF for two nets running parallel with minimum DRC spacing with a length of 1μm. The simulation results indicate that crosstalk can be used to introduce bias in the TRNG and disrupt the bit distribution, figure 51.

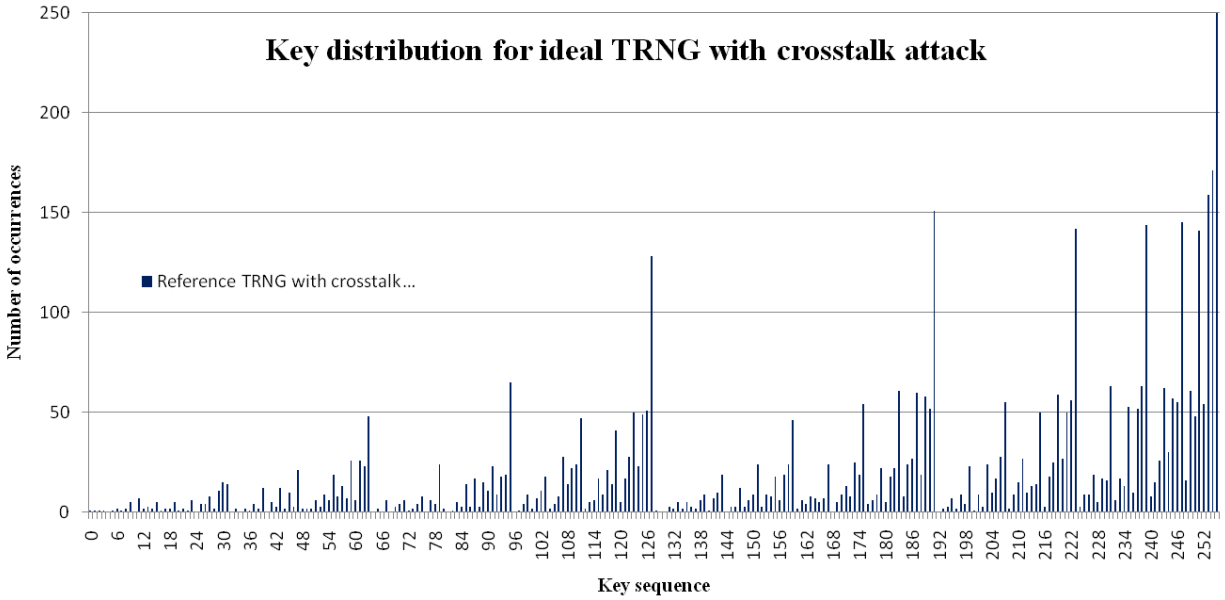


Figure 51. Distribution of 8-bit key for an ideal TRNG with crosstalk attack

6.6 Impact of attack on TRNG

Although TRNG can be a single point of failure for the entire crypto system, variation in fabrication process and hence the bias in TRNG is inevitable. Depending on the application, there could be a trade-off between the degree of randomness achieved (bit-entropy) and the over in the form of area and energy to achieve the same. Complex hashing and ciphers lead to significant overhead when compared to the negligibly small design of metastability-based TRNG. Simpler algorithmic post-processing techniques like XOR function and von Neumann corrector may not provide a near-1 entropy under all situations. Hence, t is imperative to analyze the impact of reduction in bit-entropy on the security of the system.

Table 5: Variation of byte-entropy with bit-entropy

Entropy	8bit	16bit	32bit	64bit	128bit
1	8	16	32	64	128
0.999	7.99	15.99	31.98	63.95	127.91
0.99	7.92	15.84	31.68	63.36	126.73
0.9	7.20	14.40	28.80	57.61	115.21
0.8	6.40	12.80	25.61	51.21	102.42

Table 5 shows the byte-entropy for various key-sizes with reducing bit entropy. As the bit entropy decreases, the number of effective bits in keys/seeds generated from the TRNG also decreases. For instance, for a bit entropy of 0.9, a 128-bit key generated from the biased TRNG is equivalent to a 115 bit key. In other words, for an attacker, the effort required to break the 128 bit key is equivalent to the effort required to break a 115 bit key. This is due to the bias in the TRNG. A table for the size of the key space for the same biased TRNG is as shown in table 6.

Table 6: Key space with varying bit entropy

Entropy	8bit	16bit	32bit	64bit	128bit
1	256	65536	4.29E+09	1.84E+19	3.4E+38
0.999	254.9664	65007.87	4.23E+09	1.79E+19	3.19E+38
0.99	242.2833	58701.19	3.45E+09	1.19E+19	1.41E+38
0.9	147.1066	21640.36	4.68E+08	2.19E+17	4.81E+34
0.8	84.52233	7144.024	51037080	2.6E+15	6.78E+30

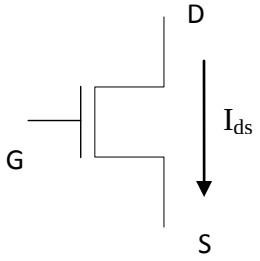
Although the bias in the TRNG reduces the effective bit size of a 128 bit key by 13 bits, the effective key space for an attacker is still 4.8e34. This is an enormously significant number in terms of the computation power required to break the key by brute force. Since process variation or variation operating temperature only increase the bias in the TRNG and not the correlation, the problem of breaking a 128 bit key wil still not be simplified for an attacker even of the TRNG is slightly biased. From [33], 84 bit is proven to be the threshold for secure key size selection. Hence, as long as the bias in the TRNG does not reduce the effective key size of a 128 bit key to below 80, the bias may be assumed to be tolerable. For large key sizes, correlation between bits of the TRNG assist the attacker more, as compared to bias in the bit stream generated. On the other hand, a 64-bit key is effectively reduced to 51 bits due to bias. This reduces the computation required by an attacker to brute force the protocol using bits from the biased TRNG. The above study provides an outlook into entropy-energy trade-offs in designing secure TRNG circuits based on the need of the application.

CHAPTER 7

STOCHASTIC MODEL FOR METASTABILITY BASED TRNG

A major challenge in design and analysis of circuits in sub-micron technologies is modeling the effect of random variations and noise. Although this can be done in HSPICE using specific Gaussian functions, a large number of sample s are required to accurately quantify the randomness of the TRNG output across various process corners. Although most analysis are performed for the worst case process variation, an estimate of the expected entropy assists in fault tolerance by choosing an appropriate post-processing technique or calibration. In this section we introduce a stochastic model for metastability based TRNG which incorporates the transistor current equations along with probabilistic description for thermal noise. The model will then be extended to analyze the effect of intra-die variation on the statistics of the TRNG followed by the impact of post-processing for various degree of device mismatch.

7.1 Thermal Noise in an isolated NMOS transistor



The drain current of an NMOS, working in saturation mode, is given by

$$\boldsymbol{I_{ds} = \frac{\beta}{2}\left(V_{gs} - V_t\right)^2} \qquad \textbf{(7.1)}$$

$$where, \beta = \frac{\mu C_{ox} W}{L}$$

In saturation mode, the drain current is governed by the gate-source voltage. Hence, any thermal noise on the gate terminal impacts the current through the transistor. Let V_{noise} be a random variable defining the thermal noise at the gate terminal of the transistor. V_{noise} has a Gaussian distribution with mean, μ_{noise} and variance, σ^2_{noise} .

$$\boldsymbol{V_{noise} \backsim N(\mu_{noise}, \sigma^2_{noise})} \qquad \textbf{(7.2)}$$

The gate-source voltage considering thermal noise is given by

$$\boldsymbol{V'_{gs} = V_{gs} + V_{noise}} \qquad \textbf{(7.3)}$$

For a constant Vgs the gate-source voltage V'gs also has a Gaussian distribution with

$$\begin{gathered} \boldsymbol{Mean,\ \mu_{gs} = \mu_{noise} + V_{gs}} \\ \boldsymbol{Variance, \sigma^2_{gs} = \sigma^2_{noise}} \qquad \textbf{(7.4)} \\ \boldsymbol{Therefore, V'_{gs} \backsim N(\mu_{gs}, \sigma^2_{gs})} \end{gathered}$$

Consider a variable, $X = \sqrt{\frac{\beta}{2}}\,(V'_{gs} - V_t)$

Then, *X* also has a Gaussian distribution with

$$Mean,\ \mu_X = \sqrt{\frac{\beta}{2}}(\,\mu_{gs} - V_t) = \sqrt{\frac{\beta}{2}}(\,\mu_{noise} + V_{gs} - V_t)$$

$$Variance, \sigma_X^2 = \frac{\beta}{2}\sigma_{gs}^2 = \frac{\beta}{2}\sigma_{noise}^2$$

$$\boldsymbol{X \backsim N\left(\sqrt{\frac{\beta}{2}}(\,\mu_{noise} + V_{gs} - V_t), \frac{\beta}{2}\sigma^2_{noise}\right)} \qquad \textbf{(7.5)}$$

7.2 Probabilistic analysis of Metastability based TRNG

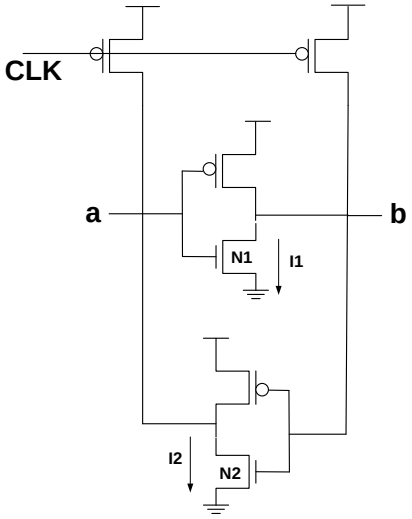


Figure 52: TRNG circuit with pull down currents

In metastability based TRNG, the NMOS devices in the cross-coupled inverters govern the output bit of the TRNG. The PMOS transistors help in retaining the state once the bit is sampled. Hence, the following mathematical formulation considers only the effect of the NMOS devices.

From the equation for drain current in (7.5),

$$\boldsymbol{I_1 = \frac{\beta_1}{2}\left(V_{gs} + V_{noise1} - V_t\right)^2}$$

$$\boldsymbol{I_2 = \frac{\beta_2}{2}\left(V_{gs} + V_{noise2} - V_t\right)^2} \qquad \textbf{(7.6)}$$

Substituting for I1 and I2 in terms of the variable X defined in the previous section (2),

$$I_1 = {X_1}^2$$

$$I_2 = {X_2}^2$$

When the design is pre-charged, both the nodes A and B are pulled to the same potential. When the pre-charge is removed, depending on the thermal noise at the gate of the two NMOS transistors, either of the output is pulled down to “0”.

For the output of the TRNG (node B pulled down), the condition is $I_1 > I_2$

$$\boldsymbol{P(bit = 0) = P(\ I_1 > \ I_2)}$$

Expressing the equation in terms of X

$$P(bit = 0) = P(\ X_1^2 > X_2^2\ )$$

$$= P(X_1 > X_2\ ) + P(X_1 < -X_2\ )$$

$$= P(X_1 > X_2\ )\ since\ X_1\ and\ X_2\ are\ always\ positive$$

$$\boldsymbol{P(bit = 0) = P(\ X_1 - X_2 > 0\ )} \qquad \textbf{(7.7)}$$

Let Y = $X_1 - X_2$

Since both X_1 and X_2 are Gaussian random variables, Y which is a linear function of two Gaussian random variables is also a Gaussian random variable with

$$Mean, \mu_Y = \ \mu_{X_1} - \mu_{X_2}$$

$$Variance, \sigma_Y^2 = \ \sigma_{X_1}^2 + \sigma_{X_2}^2$$

Since all transistors in the ideal circuit are perfectly matched, $\boldsymbol{\beta_1 = \beta_2}$

$$\mu_{X_1} = \mu_{X_2} = \mu_X$$

$$\sigma_{X_1}^2 = \sigma_{X_2}^2 = \sigma_X^2$$

Substituting these values,

$$\boldsymbol{\mu_Y} = \ 0$$

$$\boldsymbol{\sigma_Y^2 = 2\ \sigma_X^2} \qquad \textbf{(7.8)}$$

Hence,

$$P(bit = 0) = P(\ Y > 0\ )\ where\ Y \sim N(\ 0, 2\ \sigma_X^2\ )$$

$$P(bit = 0) = \ 1 - P(\ Y \leq 0\ )$$

$$= 1 - \left[\frac{1}{2} + erf\left(\frac{0-\mu_Y}{\sigma_Y}\right)\right] = 1 - \left[\frac{1}{2} + erf\left(\frac{0}{\sigma_Y}\right)\right]$$

$$\boldsymbol{P(bit = 0) = \frac{1}{2}}$$

$$\boldsymbol{P(bit = 1) = 1 - P(bit = 0) = \frac{1}{2}} \qquad \textbf{(7.9)}$$

Hence, the bits generated by an ideal TRNG (0% mismatch in devices) follows a Gaussian distribution with mean, $\mu = 0$ and variance, $\sigma = 2\frac{\beta}{2}\sigma_{noise}^2$.

In a non-ideal scenario where the two NMOS transistors are not matched either in size or threshold voltage. Assuming that transistor N_1 has a smaller channel length as compared to N_2,

$$\boldsymbol{\beta_1 > \beta_2}$$

The probability of bit *0* is given by,

$$P(bit = 0) = P(I_1 > I_2)$$

$$P(bit = 0) = P(X_1 - X_2 > 0)\ from\ equation\ (4)$$

$$P(bit = 0) = P(Y > 0)\ where\ Y = X_1 - X_2$$

Since *Y* is a linear function of two random variables,

$$Mean, \mu_Y = \mu_{X_1} - \mu_{X_2}$$

$$Hence, \boldsymbol{\mu_y} = \sqrt{\frac{\beta_1}{2} - \frac{\beta_2}{2}}\left(\boldsymbol{\mu_{noise} + V_{gs} - V_t}\right) and \quad \boldsymbol{\beta_1 > \beta_2}, \qquad \textbf{(7.10)}$$

Therefore,

$$\boldsymbol{\mu_Y = \in, where} \in > 0$$

Similarly,

$$\sigma_Y^2 = \sigma_{X_1}^2 + \sigma_{X_2}^2$$

$$\boldsymbol{\sigma_Y^2 = \sigma_{noise}^2\left[\left(\frac{\beta_1}{2} + \frac{\beta_2}{2}\right)\right]} \qquad \textbf{(7.11)}$$

Substituting these values,

$$P(bit = 0) = 1 - P(Y \leq 0)$$

$$= 1 - \left[\frac{1}{2} + erf\left(\frac{0 - \mu_Y}{\sigma_Y}\right)\right] = 1 - \left[\frac{1}{2} - erf\left(\frac{\in}{\sigma_Y}\right)\right]$$

$$\boldsymbol{P(bit = 0) = \frac{1}{2} + erf\left(\frac{\in}{\sigma_Y}\right) \ldots\ldots P(bit = 0) > \frac{1}{2}}$$

$$\boldsymbol{P(bit = 1) = \frac{1}{2} - erf\left(\frac{\in}{\sigma_Y}\right) \ldots\ldots P(bit = 1) < \frac{1}{2}}$$

Thus a mismatch in the transistor size leads to a shift in the distribution of bits generated by the TRNG, away from the ideal distribution.

7.3 Probabilistic analysis of Metastability based TRNG considering process variation

For a NMOS transistor,

$$\boldsymbol{\beta = \frac{\mu C_{ox} W}{L}}$$

$$\mu = mobility\ of\ charge\ , C_{ox} = Capacitance\ of\ the\ gate\ oxide\ ,$$

$$W, L = Width\ and\ Length\ of\ the\ transistor$$

Assuming variation only in length and other parameters to be constant,

$$\beta = \frac{k}{L} \qquad where\ k = constant$$

The length of the transistor, because of process variation has a Gaussian distribution with a mean μ_L and variance σ_L^2.

$$L \sim N(\mu_L\ , \sigma_L^2)$$

Therefore,

$$P(\beta \leq b) = P\left(\frac{k}{L} \leq b\right) = P\left(L \geq \frac{k}{b}\right)$$

$$P(\beta \leq b) = 1 - P\left(L \leq \frac{k}{b}\right)$$

$$P(\beta \leq b) = \frac{1}{2} - \text{erf}\left(\frac{k/_b - \mu_L}{\sigma_L}\right)$$

This also defines the Cumulative Distributive Function (CDF) of $\boldsymbol{\beta}$.

$$\boldsymbol{F_\beta(b) = \frac{1}{2} - \text{erf}\left(\frac{k/_b - \mu_L}{\sigma_L}\right)} \qquad \textbf{(7.12)}$$

The probability density function, PDF of $\boldsymbol{\beta}$ is the differential of the CDF. Hence, the PDF of $\boldsymbol{\beta}$ is

$$f_\beta(b) = \frac{d}{db}\left[\frac{1}{2} - \text{erf}\left(\frac{k/_b - \mu_L}{\sigma_L}\right)\right]$$

$$\boldsymbol{f_\beta(b) \sim e^{\frac{-(\frac{k}{b} - \mu_L)^2}{2\sigma_L^2}}} \qquad \textbf{(7.13)}$$

Now, considering the probability of bits "0" and "1", as a function of transistor length (in terms of $\boldsymbol{\beta}$), from equation (5),

$$\boldsymbol{P(bit = 0) = \frac{1}{2} + erf\left(\frac{\epsilon}{\sigma_Y}\right) \; and \; P(bit = 1) = \frac{1}{2} - erf\left(\frac{\epsilon}{\sigma_Y}\right)} \qquad \textbf{(7.14)}$$

where,

$$\epsilon = \left(\sqrt{\frac{\beta_1}{2}} - \sqrt{\frac{\beta_2}{2}}\right)(\mu_{noise} + V_{gs} - V_t) \; and \; \sigma_Y^2 = \sigma_{noise}^2\left[\left(\frac{\beta_1}{2} + \frac{\beta_2}{2}\right)\right]$$

Here, $\boldsymbol{\beta_1}$ and $\boldsymbol{\beta_2}$ are the "$\boldsymbol{\beta}$" values of the two NMOS transistors.

Integrating either P (bit = 0) or P (bit = 1) over the entire range of variation in length will result in the expected values of each of the probability E [P (bit = 0)] and E [P (bit = 1)] to be equal to 0.5. This does not provide any information about the effect of process variation. Hence, the bit entropy "H" as a function of the length (or β_1 and β_2) provides a better relationship between the variation in length and the randomness of the bits generated.

$$\boldsymbol{H = -P(0)\,log_2\,P(0) - P(1)\,log_2\,P(1)} \qquad \textbf{(7.15)}$$

Since P (0) and P (1) are functions of "β", the entropy "H" is also a function of "β" of the two transistors.

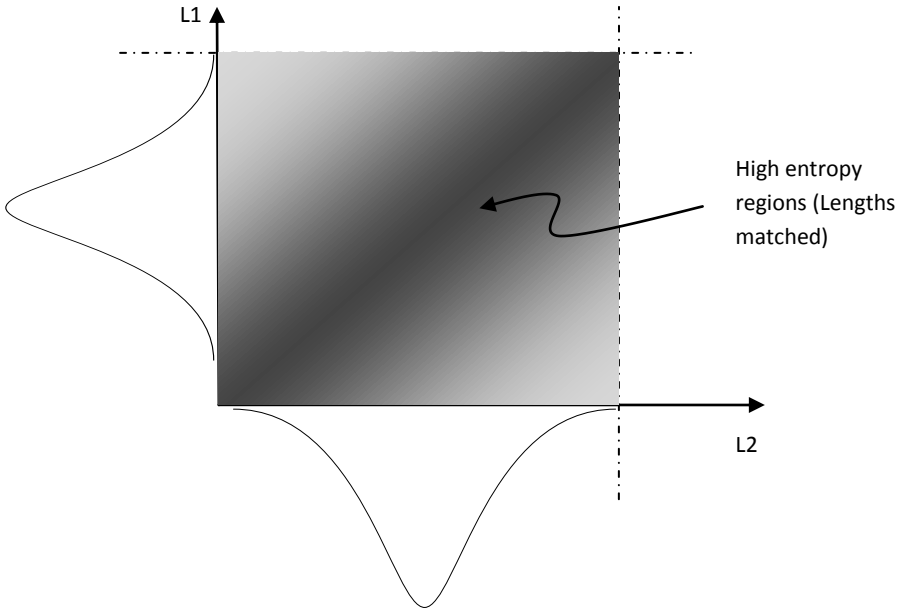


Figure 53: Distribution of entropy with variation in length

The expected value of the entropy for a given process can be expressed as the following joint PDF,

$$\boldsymbol{E[H] = \int_0^\infty \int_0^\infty H(x,y) P_{x,y}(x,y)\,dx\,dy} \qquad \textbf{(7.16)}$$

where $P_{x,y}(x,y)$ is the joint PDF of the "β" values of the NMOS devices in the cross coupled inverters.

Substituting for $P_{x,y}(x,y)$ and $H(x,y)$ from equations (7.14) and (7.15) respectively,

$$\boldsymbol{E[H] = \int_0^\infty \int_0^\infty \{ -p_0(x,y)\, log_2[p_0(x,y)] - p_1(x,y) log_2[p_1(x,y)] \}\, e^{\frac{-\left(\frac{k}{x}-\mu_L\right)^2}{2\sigma_L^2}}\, e^{\frac{-\left(\frac{k}{y}-\mu_L\right)^2}{2\sigma_L^2}}\, dx\, dy} \quad \textbf{(7.17)}$$

where, $p_0(x,y) = Probability\ of\ bit = 0\ given\ x,y$

$p_1(x,y) = Probability\ of\ bit = 1\ given\ x,y$

Using the above expression and numerical methods to solve the same, the entropy of a TRNG can be estimated for a given PDF of channel length (μ_L, σ_L^2).

7.4 Analysis of post-processing techniques

A similar analysis can be extended to post-processing techniques as well to analyze the effectiveness of the technique give the sigma variation in the process.

7.4.1 XOR Function

If XOR function is used as the post-processing technique, more than one TRNG circuits are used to feed into the XOR gate. The following analysis assumes only 2 TRNGs feeding an XOR gate. The probabilities of bits at the output of each TRNG is given by,

$$P_1(bit = 0) = \frac{1}{2} + erf\left(\frac{\epsilon_1}{\sigma_{Y1}}\right) \text{ and } P_1(bit = 1) = \frac{1}{2} - erf\left(\frac{\epsilon_1}{\sigma_{Y1}}\right)$$

$$P_2(bit = 0) = \frac{1}{2} + erf\left(\frac{\epsilon_2}{\sigma_{Y2}}\right) \text{ and } P_2(bit = 1) = \frac{1}{2} - erf\left(\frac{\epsilon_2}{\sigma_{Y2}}\right)$$

where P1 and P2 represent the probabilities of bits from each TRNG

At the output of the XOR gate,

$$P(0) = P_1(bit = 0)P_2(bit = 0) + P_1(bit = 1)P_2(bit = 1)$$

$$P(1) = P_1(bit = 0)P_2(bit = 1) + P_1(bit = 1)P_2(bit = 0)$$

The entropy as a function of lengths is given by,

$$H(l_1, l_2, l_3, l_4) = -P(0)\, log_2 P(0) - P(1)\, log_2 P(1)$$

The expected entropy is given by,

$$\boldsymbol{E[H] = \int_0^\infty \int_0^\infty \int_0^\infty \int_0^\infty H(l_1, l_2, l_3, l_4)\; e^{\frac{-(l_1-\mu_L)^2}{2\sigma_L^2}}\; e^{\frac{-(l_2-\mu_L)^2}{2\sigma_L^2}}\; e^{\frac{-(l_3-\mu_L)^2}{2\sigma_L^2}}\; e^{\frac{-(l_4-\mu_L)^2}{2\sigma_L^2}}\; dl_1\, dl_2\, dl_3\, dl_4} \quad \textbf{(7.18)}$$

7.4.2 von Neumann corrector

The von Neumann corrector reads pairs of consecutive bits from the TRNG and outputs a valid bit only if the bit pair has different polarities. At the output of the TRNG, the probability of the bits are given from equation (7.14),

$$P(bit = 0) = \frac{1}{2} + erf\left(\frac{\in}{\sigma_Y}\right) \text{ and } P(bit = 1) = \frac{1}{2} - erf\left(\frac{\in}{\sigma_Y}\right)$$

At the output of the von Neumann corrector,

$$P(0) = P(bit = 0)P(bit = 1)$$

$$P(1) = P(bit = 1)P(bit = 0)$$

Hence, *P(0) = P(1)* and theoretically the entropy of the output *H = 1*. The more significant analysis of the von Neumann correction is the degradation in the output bit rate for varying device mismatch.

$$P(valid\ bit) = P(bit = 0)P(bit = 1)$$

$$P(\ valid\ bit) = \left[\frac{1}{2} + erf\left(\frac{\in}{\sigma_Y}\right)\right]\left[\frac{1}{2} - erf\left(\frac{\in}{\sigma_Y}\right)\right]$$

$$P(\textbf{valid bit}) = \left[\frac{1}{4} - \left(erf\left(\frac{\in}{\sigma_Y}\right)\right)^2\right] \quad \textbf{(7.19)}$$

For an ideal TRNG, $\in = 0$ and hence *P(valid bit) = 1/4*. This follows the ideal scenario. For a biased TRNG, the expected bit rate is given by,

$$E[\textbf{bit rate}] = \int_0^\infty \int_0^\infty \left[\frac{1}{4} - \left(erf\left(\frac{\in}{\sigma_Y}\right)\right)^2\right] e^{\frac{-(l_1-\mu_L)^2}{2\sigma_L^2}} e^{\frac{-(l_2-\mu_L)^2}{2\sigma_L^2}} dl_1\, dl_2 \quad \textbf{(7.20)}$$

$$where \in = \left(\sqrt{\frac{\beta_1}{2}} - \sqrt{\frac{\beta_2}{2}}\right)(\mu_{noise} + V_{gs} - V_t)$$

7.5 Implementation and Results

The stochastic model was implemented in MatLab. Stratified sampling technique was used to analyze the TRNG circuit under various degree of on-chip variation. The length of the NMOS devices was swept linearly from a value equal to -3σ to a value equal to +3σ. The entropy of the TRNG was estimated based on the equation 7.14 and 7.15. The TRNG is affected more by the relative variation in the pull down devices of the two inverters rather the absolute variation. Hence, maximum entropy is observed when the devices are exactly matched and the entropy decreases with increasing mismatch between the devices. The entropy distribution plot shows the estimated entropy for variation in L_{eff} of the NMOS devices in the two inverters. It can be observed that an entropy of 1 is achieved whenever the L_{eff} values of the two devices match. In reality, the variation in L_{eff} has a Gaussian distribution and hence the probability of a particular value of L_{eff} reduces as the sample moves away from the mean value of 17nm. As a result, the estimated entropy was weighted based on the probability of the variation of length for a given Gaussian distribution of $N(\mu_L, \sigma^2_L)$. This results in a weighted entropy distribution which is dependent on the degree of L_{eff} variation ($\sigma^2_{L)}$.

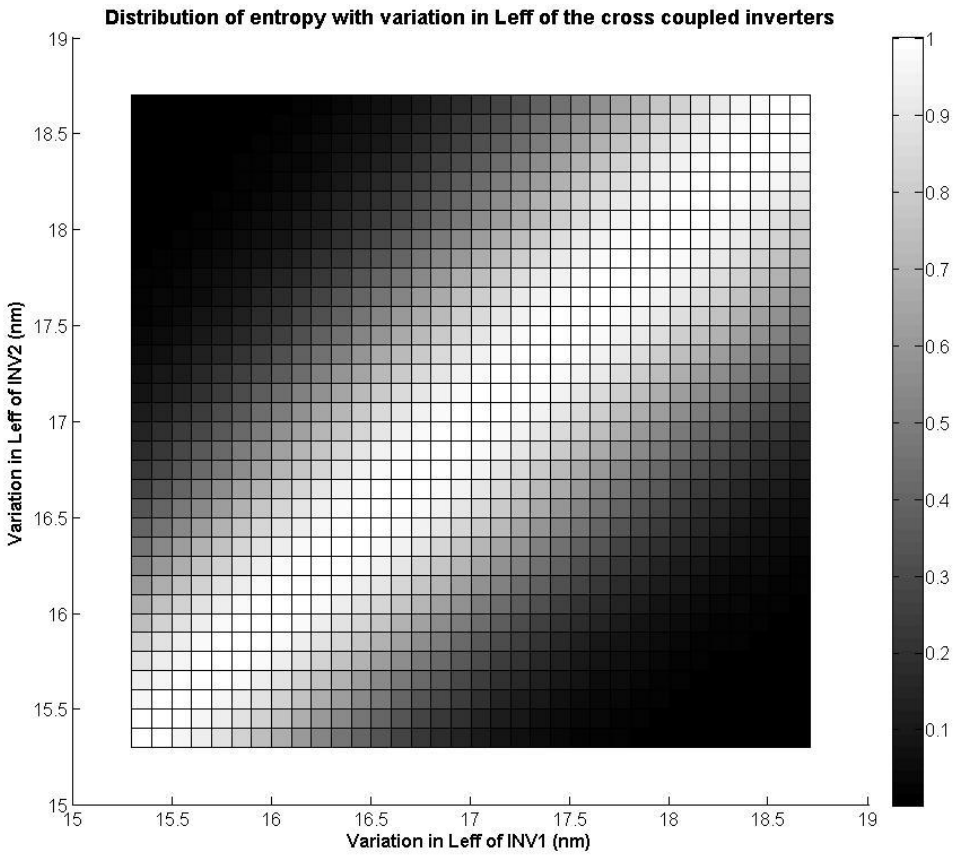


Figure 54: Distribution of entropy for variation in L_{eff}

The weighted distribution of entropy for 3σ variation in L_{eff} equal to 5% and 10% are shown in figure 47 and figure 48. A larger sigma in variation of length results in a greater probability of larger mismatch. In this case, the probability of a 5% mismatch in the two NMOS devices is higher if 3σ equals 10% than when 3σ variation equals 5%. For a given process (ie. $N(\mu_L, \sigma^2_L)$), the expected entropy is estimated as,

$$\boldsymbol{E(\mu_L, \sigma_L) = \sum_{len_1 = \mu_L - 10\%}^{len_1 = \mu_L + 10\%} \sum_{len_2 = \mu_L - 10\%}^{len_2 = \mu_L + 10\%} H(l_1, l_2)\, P(l_1 = len_1, l_2 = len_2)}$$

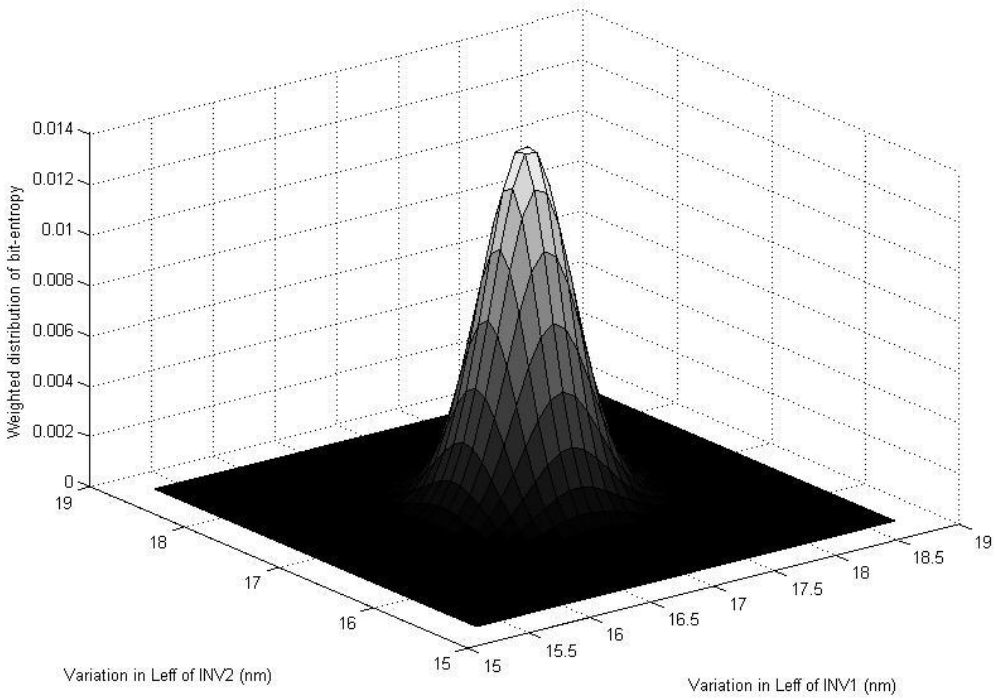


Figure 55: Weighted distribution of bit-entropy (3-sig Leff variation = 5%)

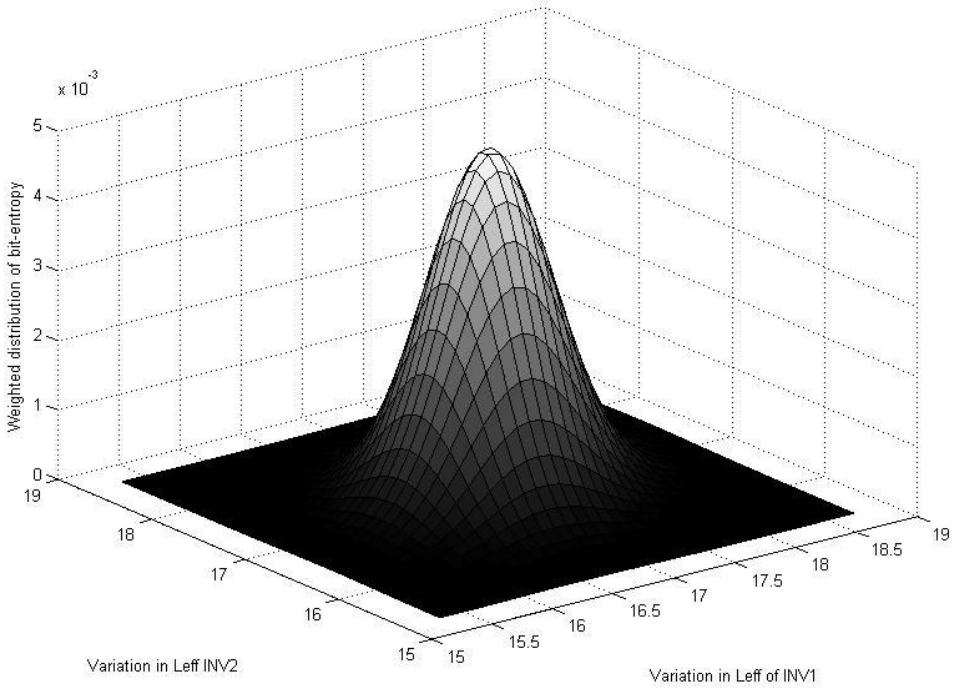


Figure 56: Weighted distribution of bit-entropy (3-sig Leff variation = 10%)

A similar analysis was extended to TRNG with XOR function and von Neumann correction as post-processing The expected entropy plotted against different process corners (varying values of σ_L) for a TRNG without correction and with post-processing techniques is as shown in fig 57. The plot indicates that post-processing techniques provide efficient correction (with minimal overhead in bit rate in case of von Neumann correction) for 3σ variation values around 2-3%. Beyond this, the expected entropy starts to decrease and further correction or redundancy may be required.

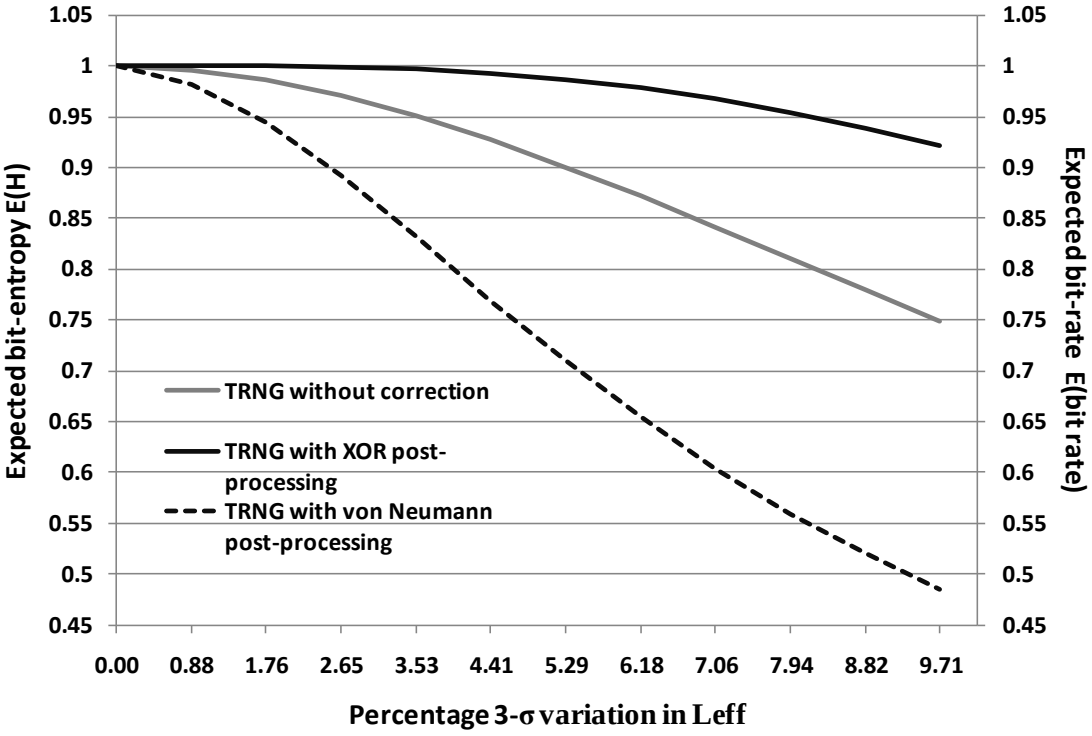


Figure 57: Expected entropy/bit rate with different sigma variation in process

Thus, the stochastic model provides an estimate of the entropy for a given process. Although the estimation lacks the accuracy of SPICE simulation which incorporates the various Short Channel Effects (SCE), it provides a fair comparison of the entropy extraction mechanisms with

significantly lower simulation effort. A comparison of the expected entropy values obtained from the stochastic model and spice simulations is as shown in fig 58.

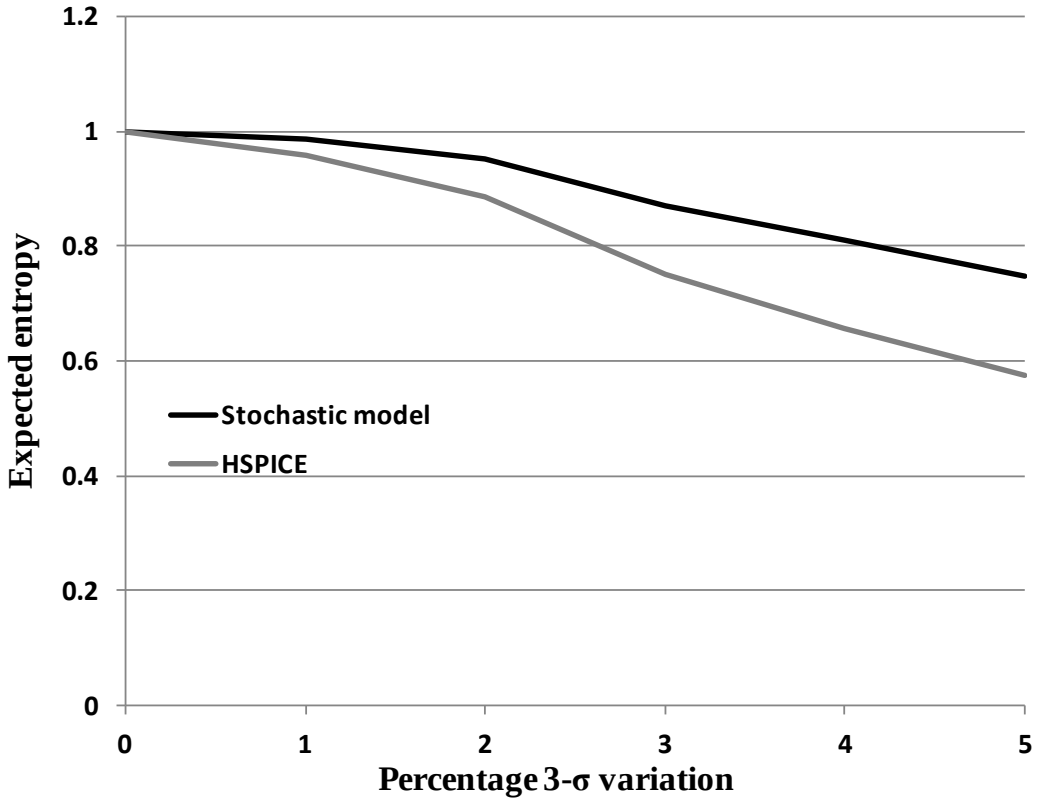


Figure 58: Comparison of stochastic model with HSPICE simulation

CHAPTER 8

CONCLUSIONS

On chip True Random Number Generators form a very critical part of cryptographic applications. With advent in technology, the TRNG circuit efficiency is affected by a number of factors like fabrication process, operating temperature and voltage. Traditional post-processing techniques may not be sufficient to mitigate these variations and ensure randomness in the bits generated.

In this thesis, a study of the effect of process variation on the bit entropy of metastability based TRNG has been presented. A comparison of the traditional post-processing techniques with circuit calibration mechanism shows that circuit level tuning provides better flexibility in terms of correction and the energy overhead. Further, the effect of variation in operating conditions has been discussed, which serve as a motivation to enhance the circuit calibration into a self-calibration mechanism. A sub-vdd pre-charge technique is introduced to render the TRNG circuit more tolerant to process variation. Pre-charging the TRNG to a voltage lesser than vdd can provide upto 2X improvement in bit-entropy for worst case device mismatches with no impact on the bit rate. A hybrid self-calibration technique is introduced using a combination of one time circuit calibration for coarse calibration and continuous algorithmic entropy extraction to compensate for finer mismatch. Different attack models were analyzed for a secure design of TRNG. It was observed that an attacker can mount an active attack on the TRNG by gaining control over global nets like supply and clock. Potential protection techniques were discussed to secure the TRNG against attacks. Finally, a stochastic model for the TRNG has been presented including a probabilistic analysis of TRNG in the presence of random process variation.

We acknowledge the support of NSF grant for **“Ultra-wideband Radio for Low-Power Security”** and SRC funding for **“Sub-45nm Circuit Design for True Random Number Generation and Chip Identification”** towards this work.

APPENDIX

SIMULATION ENVIRONMENT

One of the major challenges in simulation based research of TRNG is the development of the simulation environment itself. A TRNG basically extracts randomness from a truly random source, a source that cannot be modeled. Hence, results based on a simulation environment cannot be expected to be as accurate as the actual hardware itself.

But, simulation based research provides flexibility to the researcher to study the behavior of the circuit across a wide range of process parameters and operating conditions. Test chips fabricated to validate designs come in few numbers. The sample is not big enough to observe varied process variations, more so in works that rely heavily on the study of process variation. Further, it is a complex process to analyze the chip under varied operating conditions like temperature and voltage. Although the accuracy of the simulation results are limited by the quality of the transistor models and the tool used for simulation, the results generally provide a reasonable outlook to the behavior of the design under a varied set of constraints.

In the current work, HSPICE is used to simulate the circuit over a wide range of process variation and operating temperature. The source of randomness, thermal noise is modeled using the Gaussian function "GAUSS" in HSPICE. The methodology used here is based on the fact that once the pre-charge on inputs of the cross-coupled inverters are released, both the inputs are at the same potential of 'vdd'. But, depending on the differential thermal noise, one of the inputs drives its corresponding NMOS to an ON state, thereby sinking the current and driving its output to a state '0'. Hence, it is the differential voltage above the pre-charge voltage that decides the state of the TRNG.

To mimic this behavior, in the simulation model, each input of the cross-coupled inverter is pre-charged to a different voltage at each cycle of the simulation. Since thermal noise is seen to have a Gaussian distribution, the pre-charge signal is also modeled to have a Gaussian distribution with a mean value equal to the 'vdd' and a 3-σ variation of 50mV.

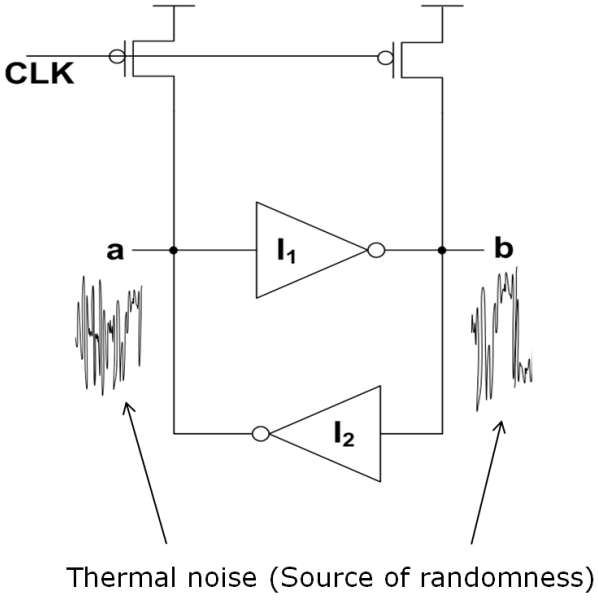


Figure 59. TRNG circuit extracting randomness from thermal noise

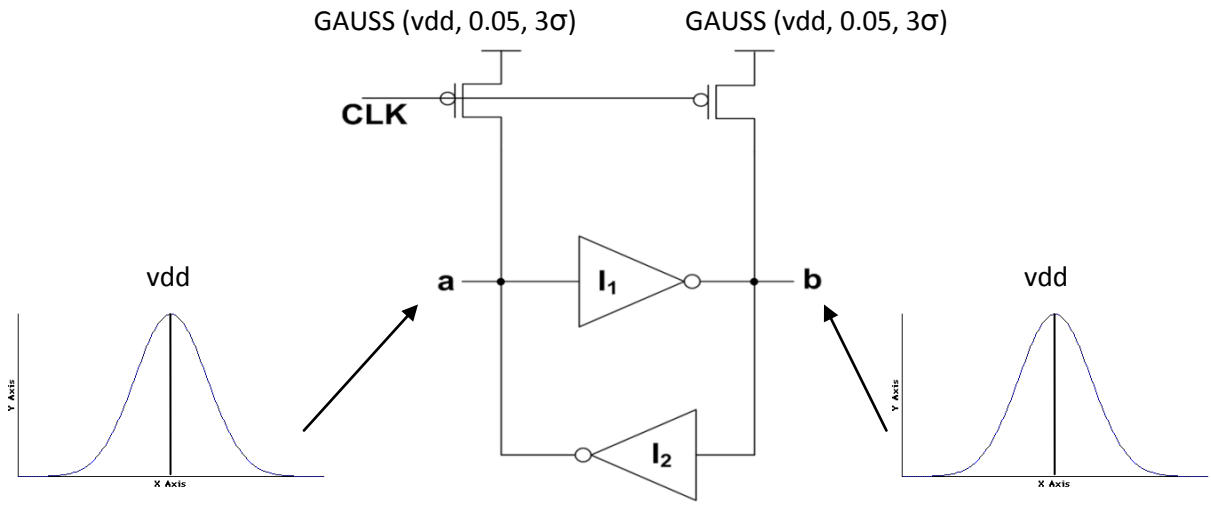


Figure 60. TRNG circuit modelled in spice with varied pre-charge potential to mimic the effect of thermal noise

Based on the mean and variance values specified, the HSPICE tool generates a sequence of data that fits a Gaussian curve. But, since it is based on an algorithm, the random values generated are

pseudo and not truly random. In other words, the data generated by the "GAUSS" function is deterministic. But, from a simulation point of view, it is desirable that the given input matches the expected noise distribution, but at the same time is repeatable over multiple runs. Hence, any optimization made to the design can be verified using the same set of input data. Although the "GAUSS" function in HSPICE basically generates deterministic bits, because of the Gaussian distribution of data, the above methodology provides a fairly close model of true thermal noise.

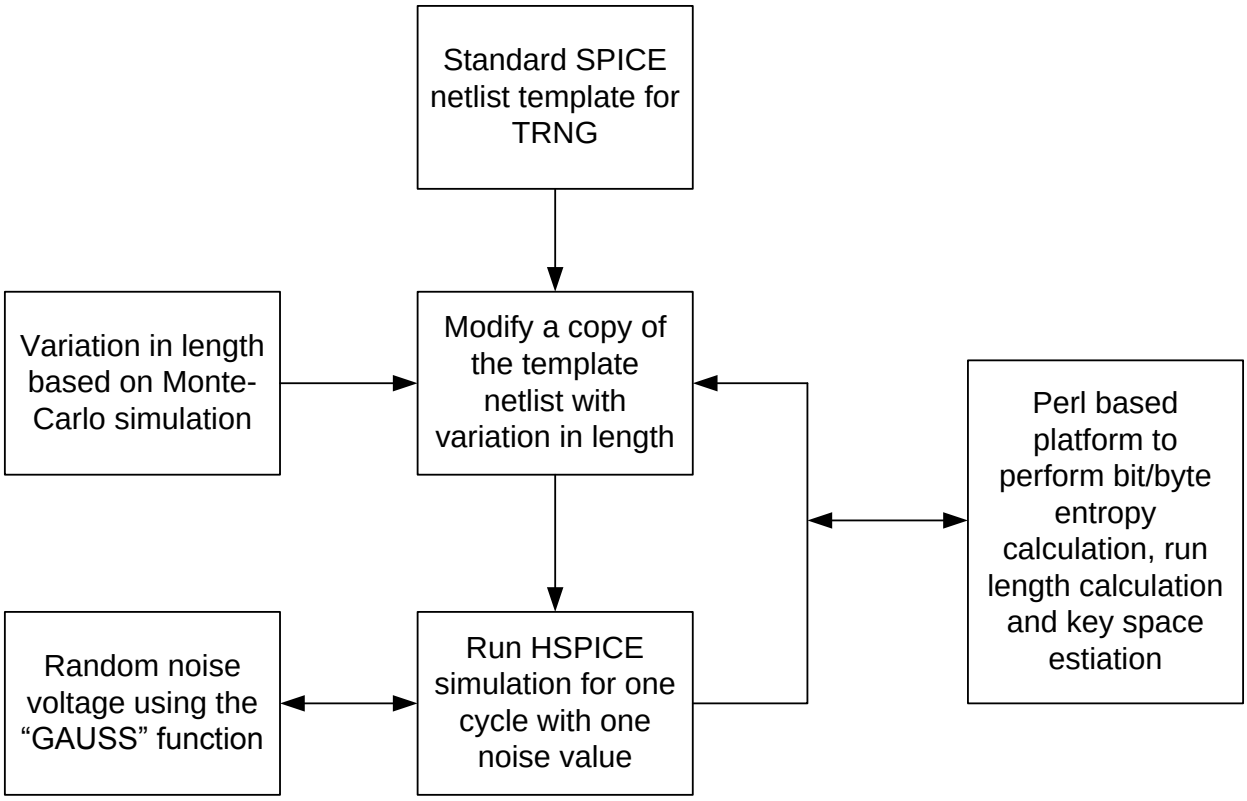


Figure 61. HSPICE and PERL based simulation platform for study of TRNG

The simulation platform built using PERL and encompassing HSPICE simulation setup is as shown in figure 48.

BIBLIOGRAPHY

[1] N. Thamrin, G. Witjaksono, A. Nuruddin, and M. Abdullah, "A Photonic-based Random Number Generator for Cryptographic Application," Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD '08. Ninth ACIS International Conference on, 2008, pp. 356-361.

[2] P. Kocher B. Jun, "The Intel Random Number Generator", in Cryptography Research Inc. White Paper Prepared For Intel Corporation, 1999

[3] C. Pyo, S. Pae, and G. Lee, "DRAM as source of randomness," Electronics Letters, vol. 45, 2009, pp. 26-27.

[4] 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, pp. 109-119.

[5] V. Fischer, F. Bernard, N. Bochard, and M. Varchola, "Enhancing security of ring oscillator-based trng implemented in FPGA," Field Programmable Logic and Applications, 2008. FPL 2008. International Conference on, 2008, pp. 245-250.

[6] N. Bochard, F. Bernard, and V. Fischer, "Observing the Randomness in RO-Based TRNG," Reconfigurable Computing and FPGAs, 2009. ReConFig '09. International Conference on, 2009, pp. 237-242.

[7] O. Cret, A. Suciu, and T. Gyorfi, "Practical Issues in Implementing TRNGs in FPGAs Based on the Ring Oscillator Sampling Method," Symbolic and Numeric Algorithms for Scientific Computing, 2008. SYNASC '08. 10th International Symposium on, 2008, pp. 433-438.

[8] "Evaluation of VIA C3 Nehemiah Random Number Generator", White paper by Cryptographic Research Inc., 2003

[9] 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.

[10] C. Tokunaga, D. Blaauw, and T. Mudge, "True Random Number Generator With a Metastability-Based Quality Control," Solid-State Circuits, IEEE Journal of, vol. 43, 2008, pp. 78-85.

[11] "A Statistical Test Suits for Random and Pseudorandom Number Generators for Cryptographic Applications," 2008.

[12] G. Geannopoulos and X. Dai, "An adaptive digital deskewing circuit for clock distribution networks," Solid-State Circuits Conference, 1998. Digest of Technical Papers. 1998 IEEE International, 1998, pp. 400-401.

[13] 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.

[14] 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.

[15] 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.

[16] J. Rabey, A. Chandrakasan, and B. Nikolic, Digital Integrated Circuits - A design Perspective, Pearson Education, 2008.

[17] BSIM4.3.0 MOSFET Model, Department of Electrical Engineering and Computer Science, University of California, Berkeley.

[18] S. Srinivasan, S. Mathew, R. Ramanarayanan, F. Sheikh, M. Anders, H. Kaul, V. Erraguntla, R. Krishnamurthy, and G. Taylor, "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.

[19] J. Boyar, Inferring Sequences Produced by Pseudo-Random Number Generators, *Journal of the ACM vol. 36*, January 1989, pp.129-141.

[20] A. T. Markettos and S. Moore, "The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators", in CHES 2009.

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

[22] 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.

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

[24] 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.

[25] 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.

[26] 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.

[27] D. Tadesse, J. Grodstein, and R. Bahar, “AutoRex: An automated post-silicon clock tuning tool,” ITC 2009.

[28] 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

[29] 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.

[30] 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.

[31] W. 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.

[32] J. Kelsey, B. Schneier, D. Wagner and C. Hall, “Cryptanalytic Attacks on Pseudorandom Number Generator”, in 5th International Workshop in Fast Software Encryption, FSE '98, Paris, France,1998

[33] “ECRYPT II Yearly Report on Algorithms and Keysizes”, European Network of Excellence in Cryptology II, 2011