

CUSTOM DESIGN OF A FULLY DIGITAL TRUE RANDOM NUMBER  
GENERATOR IN 65-NM CMOS TECHNOLOGY



by  
Ertuğ Erem

Submitted to Graduate School of Natural and Applied Sciences  
in Partial Fulfillment of the Requirements  
for the Degree of Master of Science in  
Electrical and Electronics Engineering

Yeditepe University  
2021

CUSTOM DESIGN OF A FULLY DIGITAL TRUE RANDOM NUMBER  
GENERATOR IN 65-NM CMOS TECHNOLOGY

APPROVED BY:

Prof. Dr. Uğur Çilingiroğlu  
(Thesis Supervisor)  
(Yeditepe University)

.....

Prof. Dr. Serkan Topaloğlu  
(Yeditepe University)

.....

Prof. Dr. Korkut Yeğin  
(Ege University)

.....

DATE OF APPROVAL: ....../...../2021

I hereby declare that this thesis is my own work and that all information in this thesis has been obtained and presented in accordance with academic rules and ethical conduct. I have fully cited and referenced all material and results as required by these rules and conduct, and this thesis study does not contain any plagiarism. If any material used in the thesis requires copyright, the necessary permissions have been obtained. No material from this thesis has been used for the award of another degree.

I accept all kinds of legal liability that may arise in case contrary to these situations.

Name, Last name .....

Signature .....

## ACKNOWLEDGEMENTS

I would like to express my immense gratitude to Professor Uğur Çilingiroğlu, who made me admire the field of microelectronics, gave an important aspect to my academic life, and always gave his best help.

I would like to show my appreciation to Dr. Anıl Özdemirli, who made a great contribution to me during my undergraduate years and did not spare his help in any way afterward.

I wish to extend my special thanks to my colleagues Abdullah Şahruri and Caner Toprak who did not leave me alone throughout my thesis work.

Finally, I would like to thank my family, all my friends, and especially my girlfriend İrem Sücüllü, who are always there for me, support me in every way and give their endless love.

## **ABSTRACT**

### **CUSTOM DESIGN OF A FULLY DIGITAL TRUE RANDOM NUMBER GENERATOR IN 65-NM CMOS TECHNOLOGY**

The random number generator (RNG) is an essential component for a wide range of applications. These structures, which have been used for many years, are being developed day by day. It is one of the indispensable structures in computers and smart devices, especially in today's digital world. Many design applications, games, simulation programs, password generator programs, protected communication protocols need an RNG. RNGs are generally investigated in two different categories. The first type, pseudo-random number generator (PRNG), is often software-based and works with a deterministic algorithm. It is preferred in applications that do not require security because it can be designed easily and generate random numbers with excellent statistical properties. The second type, true random number generator (TRNG), is often used for cryptographic applications. One of the most important features to look for in the TRNG is that it produces a truly unpredictable random number sequence. Therefore, it needs a non-deterministic natural source. TRNGs use an entropy source that uses physical phenomena to meet this requirement.

In this study, a custom TRNG design is presented using 65-nm CMOS technology. This design is based on metastability and is created by adding digital blocks to a structure with a dynamic comparator topology. The aim of the design is to create a circuit with a high entropy value, low power consumption, and high throughput in a small footprint as possible. It has been validated with simulations at different technology-voltage-temperature (PVT) corners to ensure that the designed circuit can operate in different conditions.

## ÖZET

### 65-NM CMOS TEKNOLOJİSİNDE TAMAMEN DİJİTAL BİR GERÇEK RASTGELE SAYI ÜRETİCİSİNİN ÖZEL TASARIMI

Rastgele sayı üreticisi (RNG), çok çeşitli uygulamalar için temel bir bileşendir. Uzun yıllardır kullanılan bu yapılar günden güne geliştirilmektedir. Özellikle dijital dünyanın hakim olduğu günümüzde, bilgisayar ve akıllı cihazlarda olmazsa olmaz yapılardan biridir. Birçok tasarım uygulamaları, oyunlar, simülasyon programları, şifre oluşturan programlar, korumalı iletişim protokolleri, bir RNG'ye ihtiyaç duyar. RNG'ler genellikle iki farklı kategoride incelenir. İlk tip olan sözde-RNG (PRNG), sıklıkla yazılım tabanlı oluşturup deterministik bir algoritmayla çalışır. Kolay bir şekilde tasarlanabilip mükemmel istatistiksel özelliklerde rastgele sayılar üretebildiği için güvenlik gereksinimi gerektirmeyen uygulamalarda tercih edilir. İkinci tip olan gerçek rastgele sayı üreticisi (TRNG) ise sıklıkla kriptografik uygulamalar için kullanır. TRNG'de aranan en önemli özelliklerden birisi, tahmin edilemeyen gerçek bir rastgele sayı dizisi üretmesidir. Bu yüzden, deterministik olmayan doğal bir kaynağa ihtiyaç duyar. TRNG'ler bu ihtiyacı karşılamak için fiziksel olguları kullanan bir entropi kaynağı kullanır.

Bu çalışmada 65-nm CMOS teknolojisi kullanılarak özel bir TRNG tasarımı sunulur. Bu tasarım metastabilite tabanlı olup, dinamik bir komparatör topolojisine sahip bir yapıya dijital bloklar eklenerek oluşturulur. Tasarımın amacı olabildiğince küçük bir alanda yüksek bir entropi değerine, düşük güç tüketimine ve yüksek çıktı verimine sahip bir devre oluşturmaktır. Tasarlanan devrenin farklı koşullarda çalışabilmesini sağlamak için farklı teknoloji-gerilim-sıcaklık (PVT) köşelerinde simülasyonlar ile doğrulanmıştır.

## TABLE OF CONTENTS

|                                               |     |
|-----------------------------------------------|-----|
| ACKNOWLEDGEMENTS.....                         | iv  |
| ABSTRACT.....                                 | v   |
| ÖZET .....                                    | vi  |
| LIST OF FIGURES .....                         | ix  |
| LIST OF TABLES.....                           | xii |
| LIST OF SYMBOLS/ABBREVIATIONS.....            | xiv |
| 1. INTRODUCTION.....                          | 1   |
| 2. PROPOSED DESIGN .....                      | 3   |
| 2.1. CIRCUIT STRUCTURE .....                  | 3   |
| 2.2. ENTROPY SOURCE.....                      | 4   |
| 2.2.1. TRNG Core Topology .....               | 4   |
| 2.2.2. Basic Operation.....                   | 6   |
| 2.2.3. Noise in Operation .....               | 13  |
| 2.3. OFFSET AND CALIBRATION.....              | 14  |
| 2.4. NOVELTY OF PROPOSED DESIGN.....          | 17  |
| 3. DESIGN STEPS.....                          | 19  |
| 3.1. DESIGN FLOW.....                         | 19  |
| 3.2. NOISE MEASUREMENT.....                   | 24  |
| 3.2.1. Periodic Noise Analysis.....           | 25  |
| 3.2.2. Transient Noise Analysis .....         | 28  |
| 3.2.3. Verification of Noise Measurement..... | 29  |
| 3.3. MINIMUM ENTROPY CALCULATION.....         | 32  |
| 3.4. STEP VOLTAGE MEASUREMENT .....           | 33  |
| 3.5. OFFSET MEASUREMENT .....                 | 37  |
| 3.6. SIZE OF SELF-CALIBRATING LOOP.....       | 40  |
| 3.7. TIMING AND CLOCK DELAYS .....            | 41  |
| 4. TRNG CIRCUIT DESIGN.....                   | 45  |
| 4.1. TRNG CORE .....                          | 45  |

|        |                                   |    |
|--------|-----------------------------------|----|
| 4.2.   | LOGIC GATES.....                  | 45 |
| 4.3.   | STAGED BUFFERS.....               | 46 |
| 4.4.   | FLIP-FLOPS .....                  | 49 |
| 4.4.1. | D-Type Flip-Flop (Register).....  | 49 |
| 4.4.2. | JK Flip-Flop.....                 | 51 |
| 4.5.   | SELF-CALIBRATING LOOP.....        | 52 |
| 4.5.1. | Custom Up-Down Counter .....      | 52 |
| 4.5.2. | NMOS Parallel Legs .....          | 55 |
| 4.6.   | CORRELATION SUPPRESSOR.....       | 56 |
| 4.6.1. | 6T-XOR Gate.....                  | 57 |
| 4.6.2. | SISO Shift Register.....          | 58 |
| 4.6.3. | SIPO Shift Register.....          | 59 |
| 4.6.4. | PIPO Shift Register.....          | 59 |
| 4.6.5. | Frequency Divider .....           | 60 |
| 4.7.   | CLOCK DELAYS .....                | 61 |
| 4.7.1. | Clock Delay Element.....          | 61 |
| 4.7.2. | Clock Delay Circuit .....         | 63 |
| 4.8.   | DESIGN CHARACTERISTICS.....       | 64 |
| 4.8.1. | Fixed Common-Mode Voltage .....   | 65 |
| 4.8.2. | Varying Common-Mode Voltage ..... | 68 |
| 4.9.   | TRNG CIRCUIT LAYOUT .....         | 70 |
| 5.     | VERIFICATION .....                | 73 |
| 5.1.   | POST-LAYOUT SIMULATION .....      | 73 |
| 5.1.1. | Timing Diagram.....               | 73 |
| 5.1.2. | Offset Compensation Test .....    | 76 |
| 5.2.   | RANDOMNESS TEST.....              | 81 |
| 6.     | CONCLUSION .....                  | 85 |
| 6.1.   | WORK SUMMARY .....                | 85 |
| 6.2.   | COMPARISON WITH OTHER WORKS ..... | 85 |
|        | REFERENCES .....                  | 87 |
|        | APPENDIX A.....                   | 90 |

## LIST OF FIGURES

|                                                                                          |    |
|------------------------------------------------------------------------------------------|----|
| Figure 2.1. General structure of proposed circuit design.....                            | 3  |
| Figure 2.2. (a) Original Strong-Arm Latch, (b) Modified Strong-Arm Latch.....            | 5  |
| Figure 2.3. Proposed TRNG core circuit .....                                             | 6  |
| Figure 2.4. Node voltages of TRNG core for cropped part of a period.....                 | 7  |
| Figure 2.5. Drain and branch currents of TRNG core in cropped part of a period.....      | 7  |
| Figure 2.6. Reset phase .....                                                            | 8  |
| Figure 2.7. Phase-E1 (First phase of evaluation).....                                    | 9  |
| Figure 2.8. Phase-E2 (Second phase of evaluation) .....                                  | 10 |
| Figure 2.9. Metastable condition of TRNG .....                                           | 11 |
| Figure 2.10. Phase-E3 (Third phase of evaluation) .....                                  | 12 |
| Figure 2.11. Effect of noise on output voltages and branch currents without offset ..... | 15 |
| Figure 2.12. Effect of offset voltage on the difference of branch currents.....          | 16 |
| Figure 3.1. Flowchart diagram of entire circuit design.....                              | 23 |
| Figure 3.2. Test setup for the TRNG core noise measurement.....                          | 24 |
| Figure 3.3. PAC and PNOISE simulation results .....                                      | 30 |
| Figure 3.4. Transient noise simulation results .....                                     | 31 |
| Figure 3.5. Test setup for the TRNG core step voltage measurement.....                   | 35 |
| Figure 3.6. Test setup for the TRNG core step voltage measurement including SCL .....    | 37 |
| Figure 3.7. Test setup of the first stage for the TRNG core offset measurement .....     | 39 |

|                                                                                                  |    |
|--------------------------------------------------------------------------------------------------|----|
| Figure 3.8. Test setup of the second stage for the TRNG core offset measurement .....            | 40 |
| Figure 3.9. Clock timing diagrams .....                                                          | 44 |
| Figure 4.1. Rising edge triggered D-Type Flip-Flop (Register) with preset and clear inputs ..... | 50 |
| Figure 4.2. Positive edge triggered Master-Slave JK Flip-Flop with preset and clear inputs ..... | 51 |
| Figure 4.3. 11-Bit Custom Up-Down Counter with preset and clear inputs .....                     | 53 |
| Figure 4.4. 11-Bit NMOS Parallel Legs .....                                                      | 55 |
| Figure 4.5. Correlation Suppressor with 8-bit output .....                                       | 57 |
| Figure 4.6. 2-input 6T-XOR gate.....                                                             | 57 |
| Figure 4.7. 29-Bit SISO Shift Register with preset and clear inputs .....                        | 58 |
| Figure 4.8. 8-Bit SIPO Shift Register with preset and clear inputs .....                         | 59 |
| Figure 4.9. 8-Bit PIPO Shift Register with preset and clear inputs .....                         | 60 |
| Figure 4.10. Frequency Divider by $f/64$ .....                                                   | 60 |
| Figure 4.11. Clock Delay Element.....                                                            | 62 |
| Figure 4.12. Clock Delay Circuit.....                                                            | 64 |
| Figure 4.13. Layout of the TRNG.....                                                             | 71 |
| Figure 4.14. Layout of the TRNG represented with the circuit blocks .....                        | 72 |
| Figure 5.1. Timing diagram of the TRNG on the best corner .....                                  | 74 |
| Figure 5.2. Timing diagram of the TRNG on the nominal corner.....                                | 75 |
| Figure 5.3. Timing diagram of the TRNG on the worst corner .....                                 | 76 |
| Figure 5.4. Offset compensation test for the best corner .....                                   | 78 |

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| Figure 5.5. Offset compensation test for the nominal corner .....         | 79 |
| Figure 5.6. Offset compensation test for the worst corner.....            | 80 |
| Figure 5.7. Calibrated offset compensation test for the worst corner..... | 81 |
| Figure 5.8. Image of the post-processed 1 million bits.....               | 84 |



## LIST OF TABLES

|                                                                                                                   |    |
|-------------------------------------------------------------------------------------------------------------------|----|
| Table 3.1. Measured effects with increasing channel widths of devices in TRNG core .....                          | 20 |
| Table 3.2. Comparison of measured RMS noise results.....                                                          | 32 |
| Table 4.1. Device sizes of TRNG core .....                                                                        | 45 |
| Table 4.2. Device sizes of CMOS logic gates .....                                                                 | 46 |
| Table 4.3. Staged-buffers used for both parts of TRNG.....                                                        | 48 |
| Table 4.4. Staged-buffers used for different parts (Part A and Part B) of TRNG .....                              | 49 |
| Table 4.5. Truth table of rising edge triggered D-Type Flip-Flop with preset and clear inputs<br>.....            | 50 |
| Table 4.6. Truth table of positive edge triggered Master-Slave JK Flip-Flop with preset and<br>clear inputs ..... | 52 |
| Table 4.7. Device sizes of 2-input 6T-XOR gate .....                                                              | 58 |
| Table 4.8. Device sizes of Clock Delay Element .....                                                              | 63 |
| Table 4.9. RMS noise measurement with a fixed common-mode voltage .....                                           | 65 |
| Table 4.10. Maximum offset cancellation capability with a fixed common-mode voltage                               | 66 |
| Table 4.11. Shannon Entropy calculation with a fixed common-mode voltage.....                                     | 67 |
| Table 4.12. Offset measurement with a fixed common-mode voltage.....                                              | 67 |
| Table 4.13. RMS noise measurement with a varying common-mode voltage .....                                        | 68 |
| Table 4.14. Maximum offset cancellation capability with a varying common-mode voltage<br>.....                    | 69 |
| Table 4.15. Shannon Entropy calculation with a varying common-mode voltage.....                                   | 69 |

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| Table 4.16. Offset voltage measurement with a varying common-mode voltage ..... | 70 |
| Table 5.1. NIST test results .....                                              | 83 |
| Table 6.1. Comparison with other works.....                                     | 86 |



## LIST OF SYMBOLS/ABBREVIATIONS

|              |                                                |
|--------------|------------------------------------------------|
| $CGSO$       | Overlap capacitance per meter of channel width |
| $C_L$        | Load capacitance                               |
| $C_{ox}$     | Oxide capacitance per unit gate area           |
| $f$          | Frequency of clock signal                      |
| $G$          | Voltage gain                                   |
| $gm$         | Gate transconductance of MOSFET                |
| $H(x)$       | Shannon entropy                                |
| $I_D$        | Drain current of MOSFET                        |
| $J_{N(MAX)}$ | Saturation drive current of NMOS               |
| $J_{P(MAX)}$ | Saturation drive current of PMOS               |
| $k$          | Boltzmann constant                             |
| $L_{(min)}$  | Minimum channel length of transistor           |
| $T$          | Absolute temperature                           |
| $T$          | Period of clock signal                         |
| $t_d$        | Delay time                                     |
| $t_{eval}$   | Evaluation time                                |
| $t_h$        | Hold time                                      |
| $t_{obs}$    | Observation time                               |
| $TOX$        | Thickness of gate oxide                        |
| $t_p$        | Propagation delay                              |
| $T_{PHL}$    | High to low propagation delay                  |
| $T_{PLH}$    | Low to high propagation delay                  |
| $t_{su}$     | Setup time                                     |
| $V_{CM}$     | Common-mode voltage                            |
| $V_{DD}$     | Supply voltage of single supply voltage source |
| $V_{DS}$     | Drain-source voltage of MOSFET                 |
| $V_{GS}$     | Gate-source voltage of MOSFET                  |
| $V_{off}$    | Offset voltage                                 |
| $V_{offc}$   | Maximum offset voltage compensating capability |
| $V_{step}$   | Step voltage                                   |

|                 |                                                                  |
|-----------------|------------------------------------------------------------------|
| $V_{TN}$        | Threshold voltage of NMOS                                        |
| $V_{TP}$        | Threshold voltage of PMOS                                        |
| $W$             | Channel width of MOSFET                                          |
| $W_N$           | Channel width of NMOS                                            |
| $W_P$           | Channel width of PMOS                                            |
| $\epsilon_{ox}$ | Dielectric constant of gate oxide                                |
| $\phi$          | Clock signal                                                     |
| $\phi_H$        | High level of clock signal                                       |
| $\phi_L$        | Low level of clock signal                                        |
| $\Phi$          | Cumulative propability for standard normal distribution function |
| $\sigma_n$      | Standard deviation of noise (Noise RMS value)                    |
| $\sigma_n^2$    | Variance of noise (Noise power)                                  |
| AC              | Alternating current                                              |
| Bit             | Binary-digit                                                     |
| CDC             | Clock delay circuit                                              |
| CDE             | Clock delay element                                              |
| CDF             | Cumulative distribution function                                 |
| CMOS            | Complementary metal oxide semiconductor                          |
| DC              | Direct current                                                   |
| FF              | Flip-flop                                                        |
| JKFF            | JK flip-flop                                                     |
| MOSFET          | Metal oxide semiconductor field effect transistor                |
| NIST            | National Institute of Standards and Technology                   |
| NMOS            | N-type metal oxide semiconductor                                 |
| PAC             | Periodic small-signal AC                                         |
| PDK             | Process design kit                                               |
| PIPO            | Parallel in parallel out                                         |
| PISO            | Parallel in serial out                                           |
| PMOS            | P-type metal oxide semiconductor                                 |
| PNOISE          | Periodic noise                                                   |
| PRNG            | Pseudo random number generator                                   |

|      |                                     |
|------|-------------------------------------|
| PSD  | Power spectral density              |
| PSS  | Periodic steady-state               |
| PVT  | Process-voltage-temperature         |
| RMS  | Root mean square                    |
| RNG  | Random number generator             |
| SCL  | Self-calibrating loop               |
| SIPO | Serial in parallel out              |
| SISO | Serial in serial out                |
| TRNG | True random number generator        |
| UDC  | Up-down counter                     |
| UMC  | United Microelectronics Corporation |
| XOR  | Exclusive-OR                        |

## 1. INTRODUCTION

True random number generators are formed with entropy sources using various sources such as semiconductor device noise, oxide breakdown, nuclear decay, oscillator jitter, metastability. Four types of techniques which are direct amplification, oscillator sampling, chaotic-based, and metastability-based are commonly used in TRNG design. Some designs can also be created by using more than a single technique [1].

In the direct amplification technique, a noise source is amplified, sampled, and quantized [2-4]. This technique requires an amplifier with high gain, low flicker noise, and low offset. Additionally, the factor that the requirement to be less sensitive to temperature and deterministic noise limits this technique.

In the oscillator sampling technique, phase noise is used. A fast oscillator is sampled with a slower clock signal [5]. Here, fast and slow oscillator frequencies must be carefully chosen to achieve randomness [6]. Even though it is easy to implement, achieving sufficient randomness in this technique is difficult [7,8].

The technique using chaotic-based systems is based on discrete-time analog signal processing. In these systems, although the initial condition is known, it operates unpredictably under the influence of the noise signal [9-11]. It is possible to achieve a high data rate and low power consumption in a small area in chaotic-based systems [12,13].

Metastability-based systems, are one of the most widely used techniques. Usually, a bistable circuit is brought to the metastability state and a random stable state is provided by thermal noise. Since fully digitally designed samples have a complex circuit structure, it is unlikely to be implemented in older CMOS technologies [14]. Thanks to the new CMOS technologies, there are TRNG examples that can be implemented at very high speed, with very high entropy value, and in a small footprint by using multiple entropy sources [15]. In order to obtain a high entropy value in metastability-based systems, the offset in the entropy source must be compensated. By using an analog feedback loop, the offset can be removed and the circuit can be implemented in a smaller area than with fully digital designs [16].

The proposed design is described in Chapter 2. The general circuit structure, the entropy source used and its operation, the technique used for offset compensation are explained in

detail. In Chapter 3, which includes the design steps, the factors affecting the design, the design plan, the measurements and calculations required for the design are explained in detail. All analyzes in the simulation environment were performed using Cadence® Virtuoso Spectre. In Chapter 4, detailed TRNG design, design specifications, and layout of the entire circuit are indicated. In Chapter 5, the verification results of the design are given. In Chapter 6, the work done is summarized and compared with other works.



## 2. PROPOSED DESIGN

### 2.1. CIRCUIT STRUCTURE

The proposed design consists of four types of main blocks which are a TRNG core used as an entropy source, two Self-Calibrating Loop circuits that compensate the offset, a Correlation Suppressor operating as a post-processor, and two clock delay circuits that generate new clock signals by adding delays. Apart from these main blocks, there are also staged buffer designs that allow a faster drive of the large load capacitances that occur in the circuit. This circuit design is convenient for digital circuit design and can be implemented with a similar method in different CMOS technology processes. UMC 65-nm PDK was used for the entire circuit design and all devices have 1.2 V supply voltage, standard threshold option, and minimum length. The general structure of the proposed circuit design is shown in Figure 2.1 as subcircuit blocks.

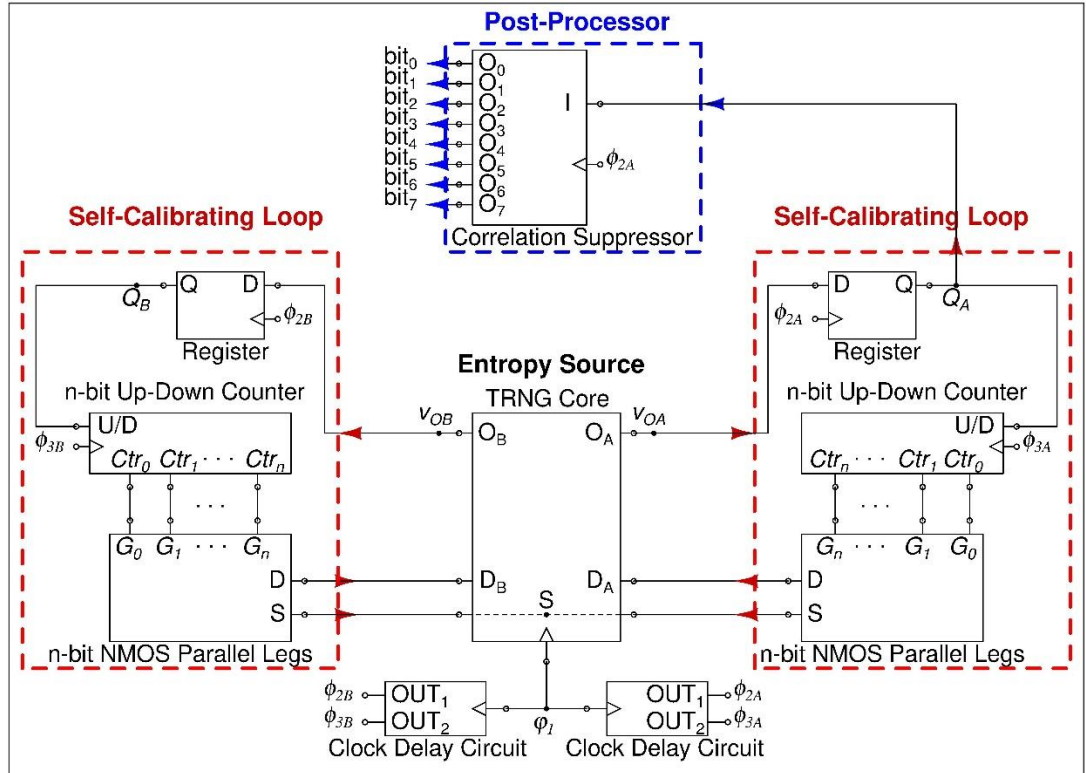


Figure 2.1. General structure of proposed circuit design

Random number generation occurs through the thermal noise generated inside the entropy source. The fact that the noise generated on one side of the core of the circuit is different from the noise generated on the other side provides true random number generation.

Mismatch during production induces an offset in the TRNG core. This offset causes the random number generation to be generated continuously bit-1 or bit-0. The Self-Calibrating Loop circuit consists of a feedback loop that dynamically compensates this offset.

Even if the TRNG circuit is properly designed, offset is eliminated, and operates with enough amount of noise, there would be a serial correlation in random numbers to be produced. Therefore, this bitstream requires a post-processing operation. The post-processing technique has been formed entirely from the correlation suppressor circuit used by Intel® [17].

The complete TRNG circuit only has one clock signal input which is used for the entropy source. However, some blocks such as registers and counters need different clock signals to operate the proposed circuit properly. Custom designed clock delay circuits meet this requirement.

## **2.2. ENTROPY SOURCE**

The entropy source of this design is based on a metastability-based true random number generator topology. The topology, simple operation, and noise in the operation of the circuit are described in Section 2.2.1, Section 2.2.2, and Section 2.2.3, respectively.

### **2.2.1. TRNG Core Topology**

TRNG core circuit is inspired by the modified Strong-Arm Latch topology [18]. This circuit is arranged to be a random number generator instead of being used as a comparator. To obtain a high entropy, it is aimed to maximize the noise that may occur in the circuit as much as possible. The electrical schematic of the original and the modified version of the Strong-Arm Latch circuit is given in Figure 2.2.

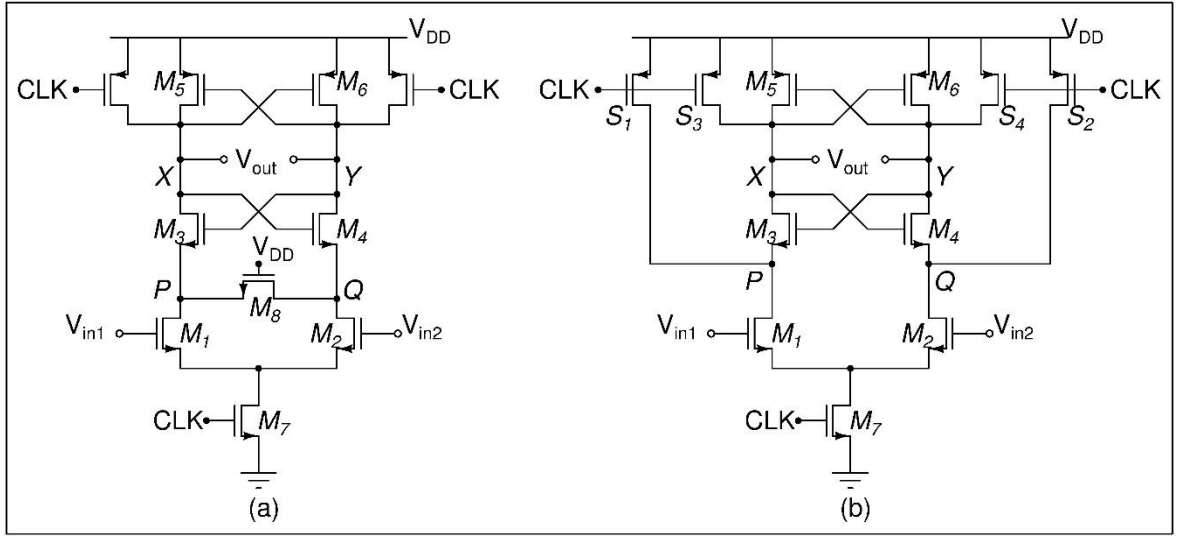


Figure 2.2. (a) Original Strong-Arm Latch, (b) Modified Strong-Arm Latch.

The proposed TRNG core circuit shown in Figure 2.3 includes two cross-coupled pairs,  $M_{1-2}$  and  $M_{3-4}$ , two control transistors,  $M_{5-6}$ , four precharge transistors,  $M_{S1-S4}$ , and a tail transistor,  $M_7$ . The gate terminals of  $M_{S1-S4}$  and  $M_7$  are controlled by a clock signal. In this circuit,  $M_{1-2}$ ,  $M_{3-4}$ ,  $M_{5-6}$ ,  $M_{S1-S2}$ , and  $M_{S3-S4}$  are matched devices, respectively. Differential input pair in Strong-Arm Latch takes part as control transistors in the proposed TRNG core circuit. Instead of applying a differential input voltage to these control transistors, only the common-mode voltage,  $V_{CM}$ , is applied to their gates.

Since the entropy source has similar behaviors with Strong-Arm Latch, it is useful to examine the simple operation of this circuit in different phases [19]. While the first phase where the clock signal is low forms the reset phase, the evaluation phase where the clock signal is high is considered in four different phases as E1, E2, E3, and E4, respectively. It is assumed that there is no offset while analyzing the operation phases. Voltages of  $CLK$ ,  $OA$ ,  $OB$ ,  $DA$ ,  $DB$ , and  $S$  nodes are performed in Figure 2.4 including all five phases for the entropy source. Moving from the  $S$  node to the supply voltage,  $V_{DD}$ , the entropy source can be split into two completely symmetrical parts. The total current generated in the right half part,  $I_A$ , and the left half part,  $I_B$ , merge at the  $S$  node, and this combined current,  $I_S$ , flows to the ground. In consideration of  $M_{1-7}$  is active in the evaluation phase, the currents generated by these transistors,  $I_{D1-7}$ , and the branch currents  $I_A$ ,  $I_B$ , and  $I_S$  are presented in Figure 2.5.

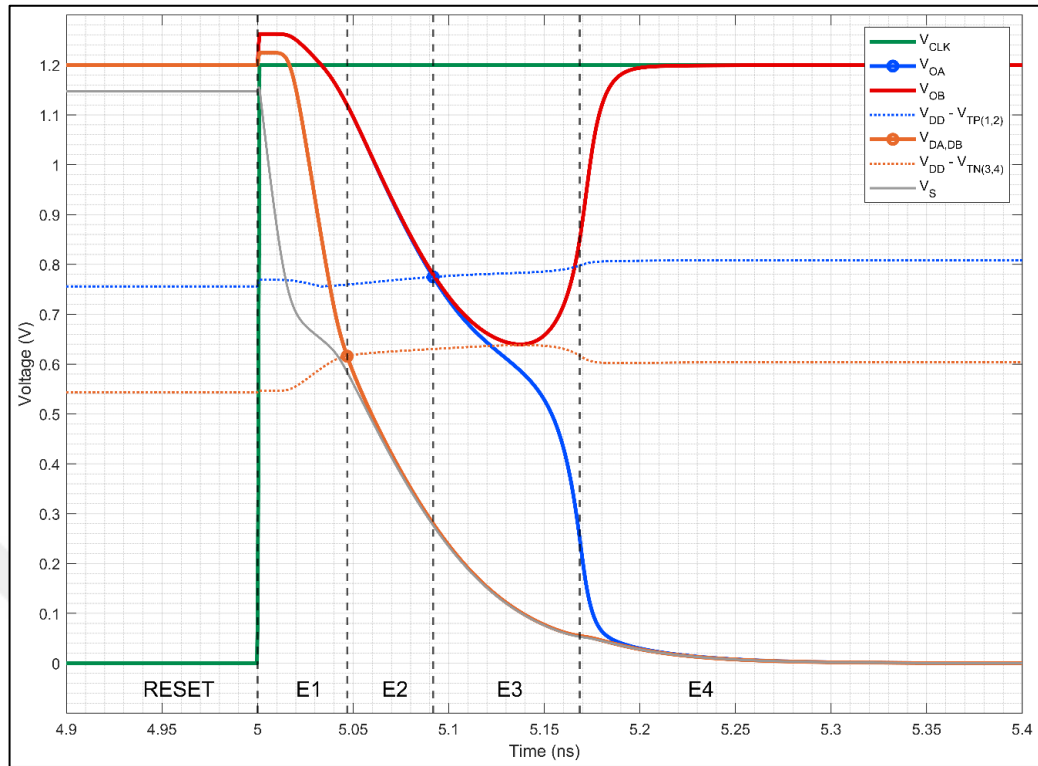


Figure 2.4. Node voltages of TRNG core for cropped part of a period

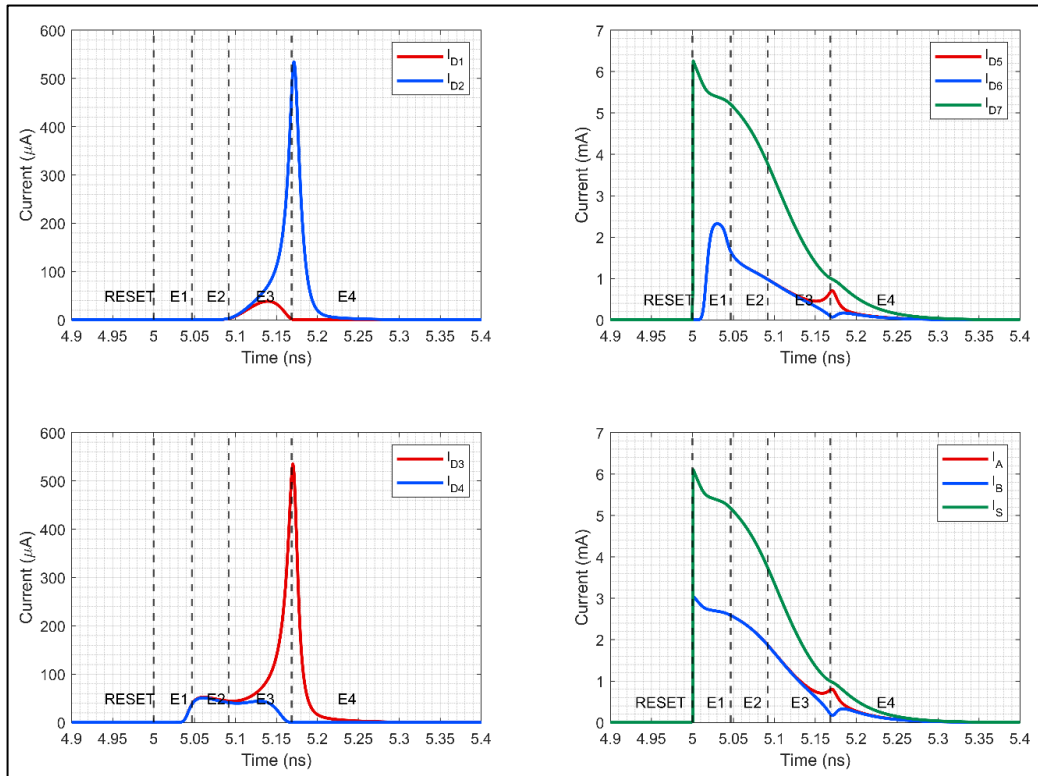


Figure 2.5. Drain and branch currents of TRNG core in cropped part of a period

In the reset phase,  $M_{S1-S4}$  PMOS transistors precharge  $OA$ ,  $OB$ ,  $DA$ , and  $DB$  nodes to  $V_{DD}$ , by receiving the ground signal to their gate terminals. Since the same ground signal also arrives at the gate terminal of  $M_7$ , this NMOS transistor is in the cut-off state and disconnects the ground connection. The  $S$  node which is the common source terminal of the control transistors is loaded to a certain voltage level depending on common-mode voltage,  $V_{CM}$ . To make each phase more understandable, the equivalent circuit after the precharge process of this phase is completed is represented by the equivalent capacitances formed at these nodes in Figure 2.6.

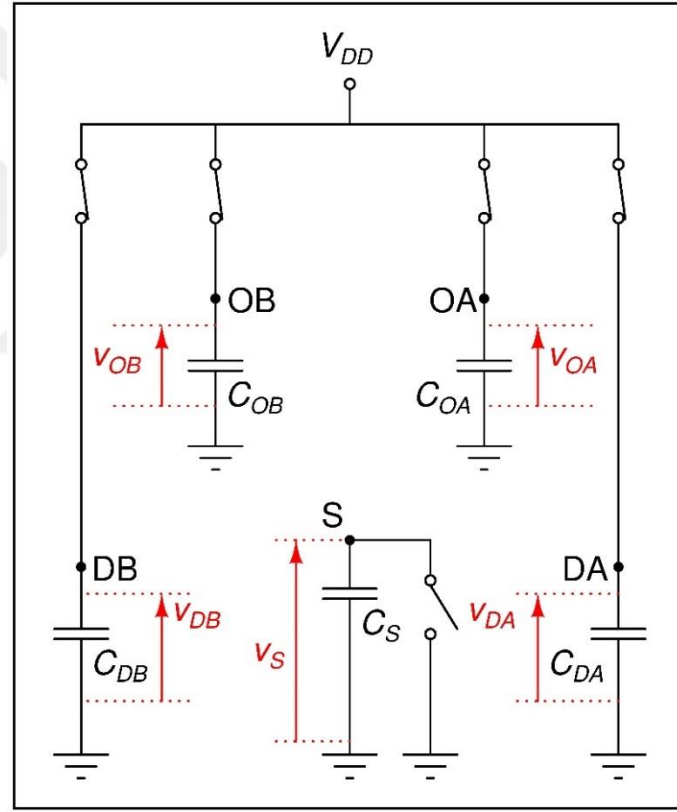


Figure 2.6. Reset phase

In phase-E1, where the clock signal rises from low to high,  $M_{S1-S4}$  precharge transistors receiving  $V_{DD}$  signal to their gates turn off and do not flow any current in this phase. On the other hand,  $M_7$  turns on and starts to discharge the capacitance on the  $S$  node. A drop in  $V_S$  causes an increase in port voltages  $V_{GS5,6}$  and  $V_{DS5,6}$  where these values stand for gate-source and drain-source voltages of  $M_{5,6}$ , respectively. Meanwhile,  $M_{5,6}$  are in conduction and start

to flow current in saturation mode. These transistors lower the voltages on  $DA$  and  $DB$  nodes while suppressing  $M_7$  that decreases  $V_S$ . Moreover,  $V_{DA}$  and  $V_{DB}$  drop rapidly while  $V_S$  falls slowly. Therefore,  $M_{5,6}$  whose drain-source voltage decreases gradually pass to the non-saturation mode. In this phase,  $M_7$  does not only act as a switch but also limits the currents to flow over  $M_5$  and  $M_6$ . Phase-E1 ends when  $V_{DA}$  and  $V_{DB}$  drop down to  $V_{DD} - V_{TN3,4}$  where  $V_{TN}$  represents the threshold voltage of the NMOS transistor. The reduced form of the circuit in this phase is represented in Figure 2.7.

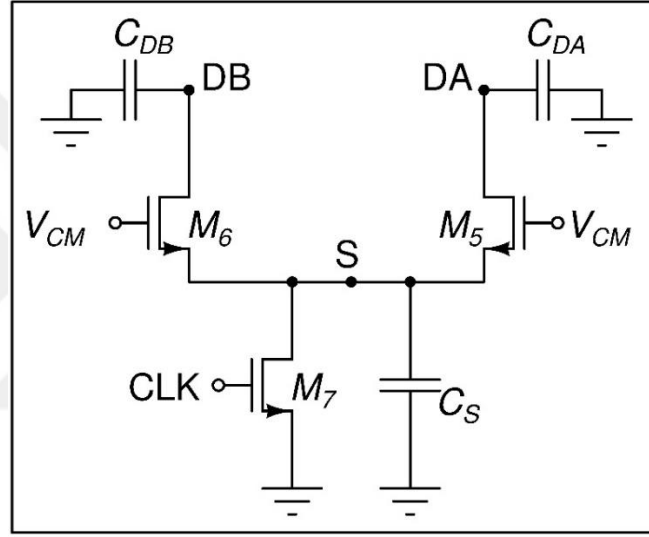


Figure 2.7. Phase-E1 (First phase of evaluation)

In phase-E2,  $M_3$  and  $M_4$  start conducting current and discharge  $V_{OA}$  and  $V_{OB}$ . Concurrently,  $M_5$ ,  $M_6$ , and  $M_7$ , which are still in conduction, continue to reduce  $V_{DA}$  and  $V_{DB}$ . This phase ends when  $V_{OA}$  and  $V_{OB}$  reach  $V_{DD} - V_{TP1,2}$  where  $V_{TP}$  represents the threshold voltage of the PMOS transistor. Figure 2.8 indicates the reduced state of the circuit in this phase with the transistors in conduction and the capacitances on these nodes.

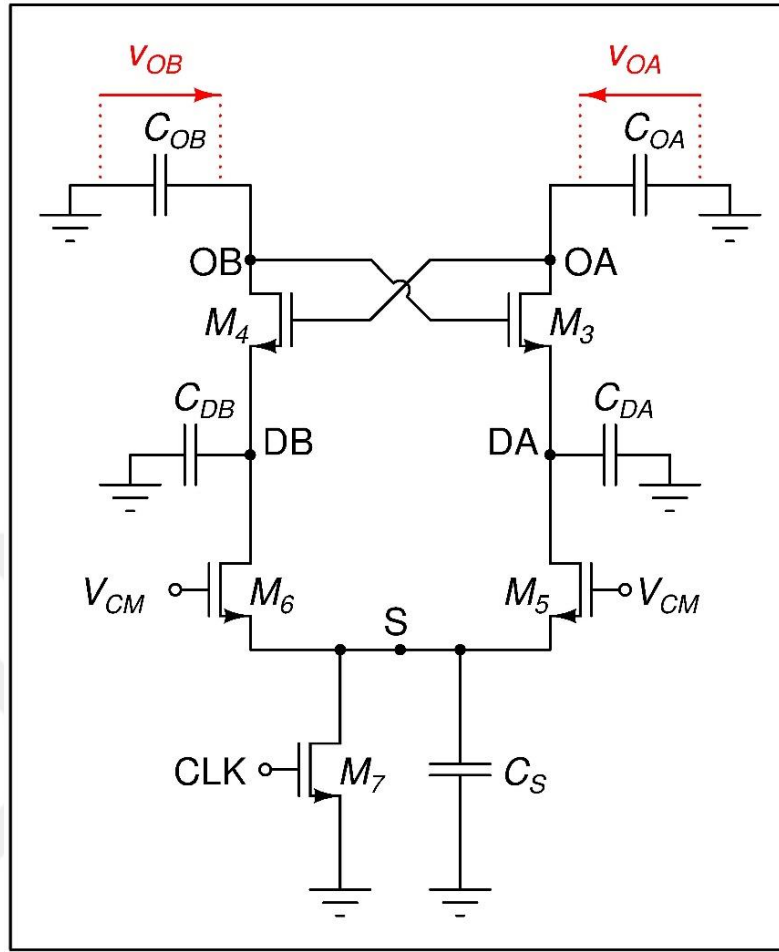


Figure 2.8. Phase-E2 (Second phase of evaluation)

In phase-E3,  $M_1$  and  $M_2$  finally turn on. A drop in  $V_{OA}$  and  $V_{OB}$  causes  $V_{GS1,2}$  to increase. With PMOS devices starting to flow current, the decrease in  $V_{OA}$  and  $V_{OB}$  is tried to be suppressed. In the ideal case where there is no offset and noise,  $V_{OA}$  and  $V_{OB}$  would have been locked at the point of metastability after falling together to a certain voltage level. Since  $M_{1,3}$  and  $M_{2,4}$  cross-coupled pairs act as inverters, the metastability point is determined by the logic threshold voltage of these cross-coupled inverters. In this metastable case where  $M_{1-7}$  still are in conduction, the circuit draws a static current by reason of the path between the supply and the ground connection is provided until this phase ends. The output voltage values of the circuit and the branch currents in a metastable condition are displayed in Figure 2.9.

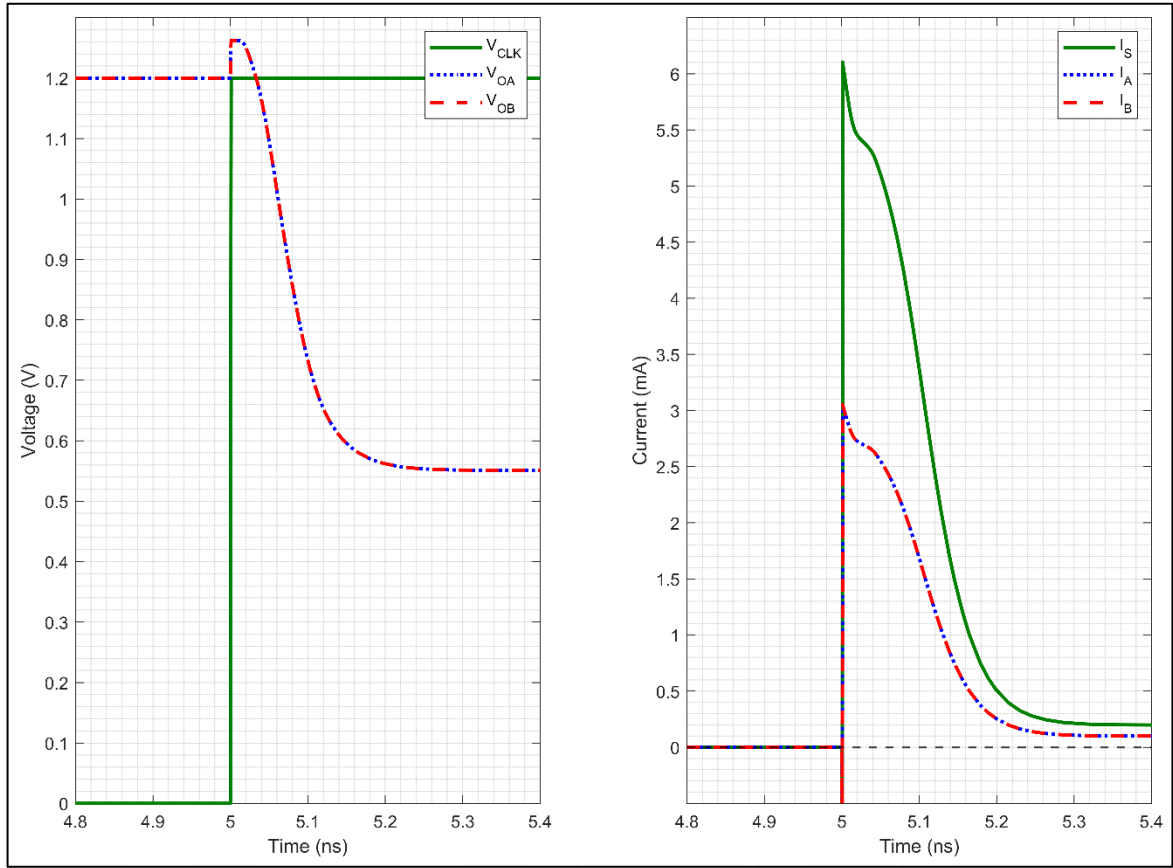


Figure 2.9. Metastable condition of TRNG

Assuming the case that the noise level at node  $OA$  is more positive than node  $OB$  around the metastability point, it causes inequality on the inputs and outputs of the cross-coupled inverters. While a slight increase of voltage level on  $V_{OA}$  due to additive noise triggers  $V_{OB}$  to decrease, falling  $V_{OB}$  also triggers  $V_{OA}$  to rise. This situation causes the outputs of TRNG to separate from each other significantly. As both voltage levels of the outputs move together until the beginning of this phase, a voltage gap begins to occur with the start of separation. Therefore, a difference emerges in the currents flowing through on both branches of TRNG. The phase-E3 is completed when the voltage difference of the outputs reaches half of  $V_{DD}$ . As in other previous phases, the reduced circuit in this phase is given in Figure 2.10.



### 2.2.3. Noise in Operation

The noise generated during the operation of the TRNG core forms the basis of the entropy source. Although there are various types of noise sources such as flicker, shot noise, the influential type is the thermal noise in this circuit. Since the proposed circuit is based on a dynamic comparator topology, it is necessary to examine the time-varying noise in different phases. A standard AC noise analysis can only be done when the circuit is in a static condition such as the reset phase. However, to analyze the noise in the evaluation phase, which has complex and dynamic characteristics, transient noise analysis or PSS/PNOISE (Periodic Steady-State / Periodic Noise) and PAC (Periodic Small-Signal AC) analyzes should be performed. The results of these two types of noise analysis measured on a dynamic comparator come out close to each other. Since transient noise simulation may take thousands of times slower than PSS/PNOISE analysis, it is more appropriate to use it for verification.

While transitioning from the reset phase to the evaluation phase, channel thermal noise generated in  $M_{S1,S2}$  that precharge  $OA$  and  $OB$  nodes are sampled on the capacitances related to these nodes. This situation creates the initial condition of the noise which is  $kT/C$  noise. The power of the noise,  $\sigma_n^2$ , varies inversely with the capacitance values formed at these nodes at a constant temperature. Therefore, keeping the sizes of  $M_{S1,S2}$  and  $M_{1-4}$  smaller affects positively for the first stage of the noise power. In evaluation phases,  $M_{5-6}$ ,  $M_{3-4}$ , and  $M_{1-2}$  being in conduction contribute to the noise power, respectively. In addition to  $kT/C$  noise, parameters such as evaluation phase transition times, transconductances of transistors, and MOS noise factor become effective. Analyzing the power of noise in each phase requires a highly sophisticated analytical approach. In order to calculate the total power of the noise in a dynamic comparator, it is necessary to sum up the variances of the noise in each phase. In these structures, generally, the input-referred noise,  $\sigma_n$ , is obtained by applying a signal to the input using PSS/PNOISE and PAC simulations. PSS/PNOISE simulation provides measuring the noise at the outputs while PAC simulation provides to measure the voltage gain between the input and the output signal. Consequently, dividing the output noise by the gain gives the RMS value of the input-referred noise [20,21].

### 2.3. OFFSET AND CALIBRATION

The device mismatch that occurs during manufacturing in entropy source shows its effect from the beginning of the evaluation phase. Considering phase-E1, a current difference occurs from both branches of the TRNG core as a result of  $M_5$  and  $M_6$  not being able to conduct equal currents to each other. This situation is not only limited to phase-E1 but also continues through  $M_{3-4}$  and  $M_{1-2}$  in phase-E2 and phase-E3. Although different offset effects can be seen in different phases, the fact that the current difference between  $I_A$  and  $I_B$  is not zero until the metastability point is a result of the equivalent offset in the circuit. If there was no offset and noise, the absolute value of this current difference,  $|I_{AB}|$ , would remain zero during the evaluation phase. As a result, a change in  $|I_{AB}|$  can be observed when a dc voltage source is connected between the cross-coupled inverters in an ideal TRNG core circuit to represent all these offset effects. Thus, a single offset parameter in terms of voltage,  $V_{off}$ , can be obtained.

In a metastable condition with noise and without offset, a small level of inequality occurs in the TRNG core due to the presence of the noise and one of the outputs reaches bit-1, while the other goes to bit-0. In this case, the output nodes whose voltage values fall together begin to separate from each other around the metastability point.  $|I_{AB}|_{(max)}$ , which is the maximum value of the magnitude of the current difference in both branches, has a certain value according to the design of the TRNG core circuit and the conditions it has. The effect of noise on  $|I_{AB}|_{(max)}$  and the output voltages is given in Figure 2.11 including five different noise seeds.

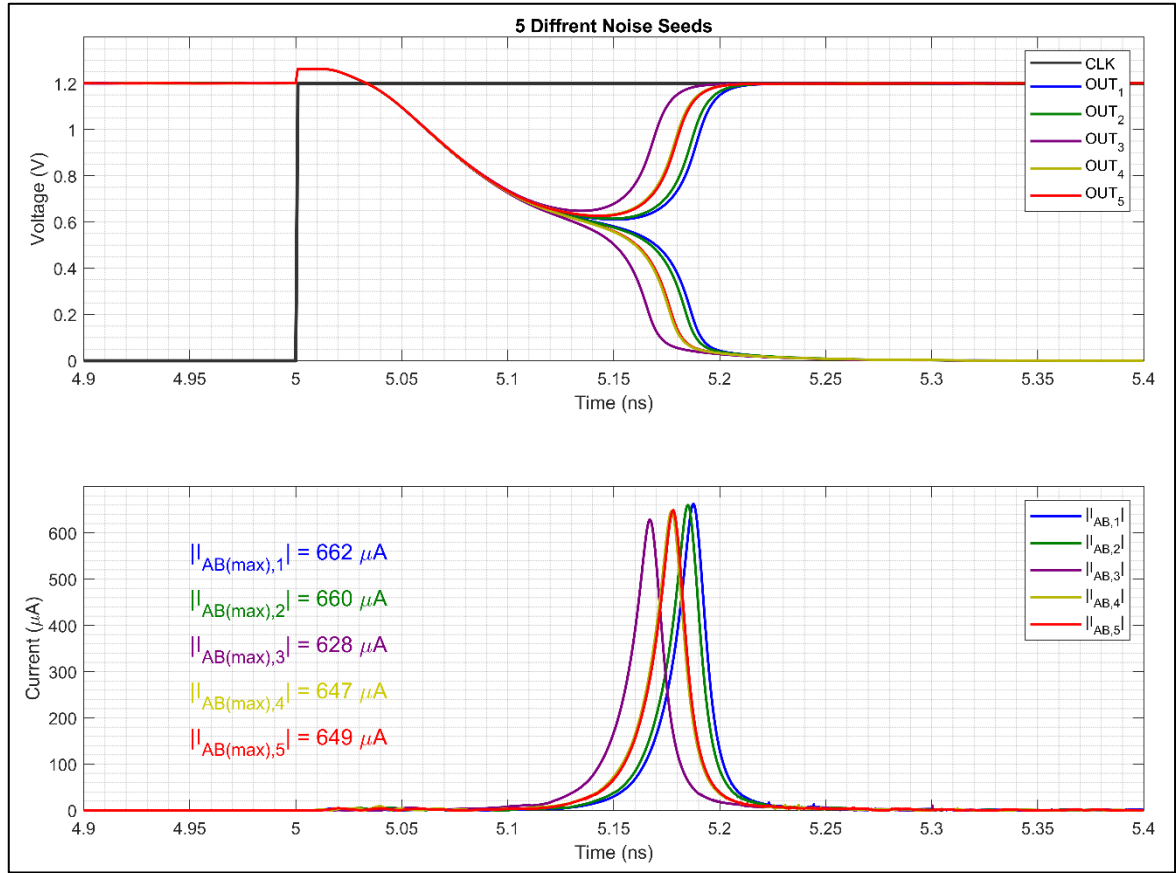


Figure 2.11. Effect of noise on output voltages and branch currents without offset

As the offset value increases in any condition,  $V_{OA}$  and  $V_{OB}$  diverge at a point farther from the logic threshold voltage level of the cross-coupled inverter, and evaluation occurs slightly faster. Thus,  $|I_{AB}|_{(max)}$  decreases when offset voltage increases. The effects of offset voltage on  $|I_{AB}|$  values are shown in Figure 2.12. In order to calculate the offset in the proposed design, Monte Carlo analysis is performed at different corners, and the point where  $|I_{AB}|_{(max)}$  is minimum should be determined. This value represents the maximum offset that can occur. Since noise can create various offset effects, it is crucial to perform these simulations in noiseless conditions. After Monte Carlo simulations, a transient simulation without noise is performed by giving parametric dc offset voltage values to the circuit for each corner. In this simulation, the value of  $V_{off}$  is recorded for the point where  $|I_{AB}|_{(max)}$  meets its maximum offset condition.

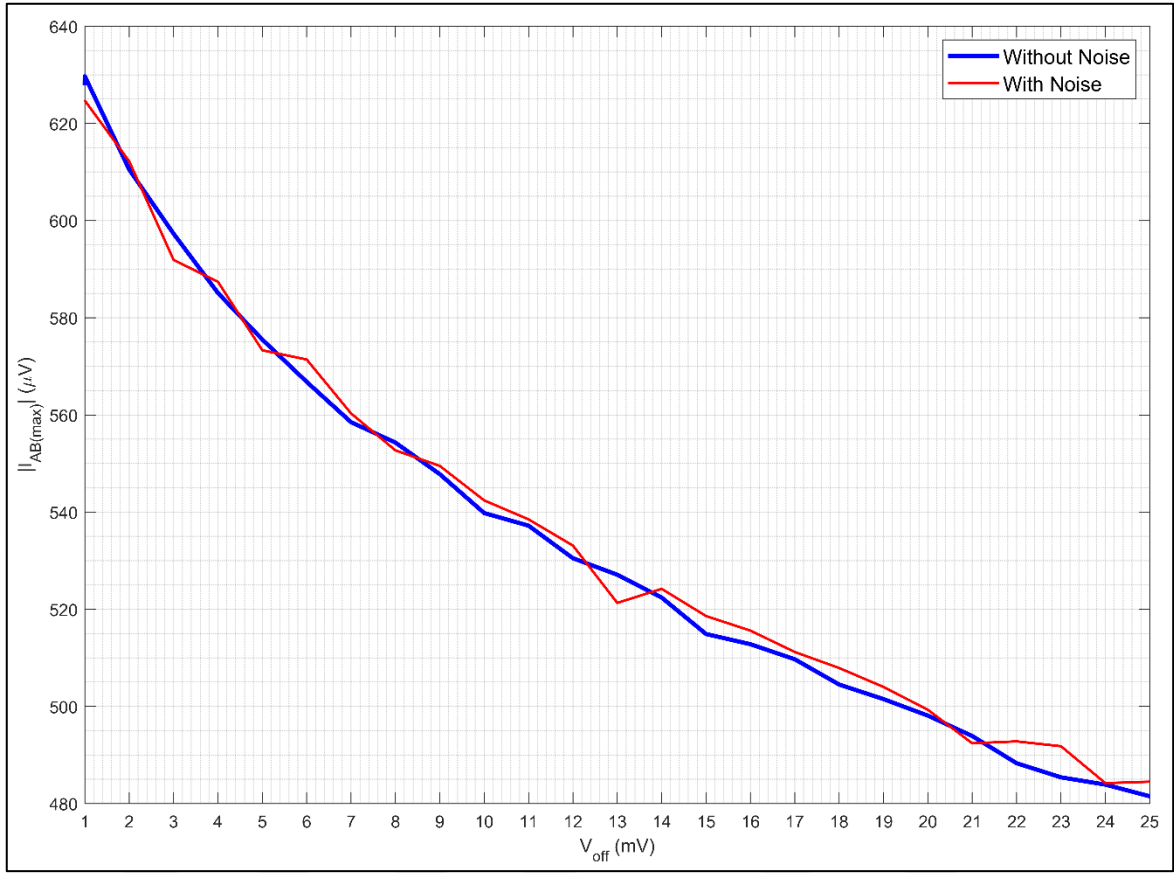


Figure 2.12. Effect of offset voltage on the difference of branch currents

The offset in the proposed circuit is compensated by changing the conductance on the paths where  $I_A$  and  $I_B$  flow. Inside the Self-Calibrating Loop (SCL), there is an array of NMOS devices designed in minimum geometry. These transistors which are called legs are connected in parallel to  $M_5$  and  $M_6$ . By activating and deactivating the legs one by one,  $I_A$  and  $I_B$  are controlled. In fact, the gate transconductances of control transistors,  $gm_5$  and  $gm_6$ , do not change. Due to the parallel connection of the legs and the control transistors, the  $gm$  of legs that are in conduction are added. Therefore, conductivity effectively increases. Since the size of a leg is very small compared to the size of  $M_{5,6}$ , activating each leg increases the total current drawn in that branch slightly. Since the effect of noise is very small beside the total offset in the circuit, it is very important to achieve the goal of equalizing the currents  $I_A$  and  $I_B$  in small steps. The effect of the step taken in each period during offset compensation on the offset voltage is represented as  $V_{step}$ . In order to achieve a high entropy,  $V_{step}$  should be smaller than  $\sigma_n$ . If the peak value of noise is less than  $V_{step}$ , the outputs in each period oscillate continuously.

When each bit-1 is generated in TRNG, one leg is enabled by the SCL while one leg is disabled for each bit-0 generation. Since opposite bits are always produced at TRNG outputs, the SCL subcircuits on both sides work opposite to each other. Therefore, as long as the total number of legs activated on either side is not zero, the value of  $V_{step}$  in each period is doubled. Assuming that all legs are deactivated in the initial state, the leg activation process starts unilaterally. Thus, each bit-1 value generated on the side where the conductivity is weaker strengthens its conductance in that branch by one step. This process continues until the offset is compensated sufficiently by one  $V_{step}$  value. After the offset compensation is completed, random number generation starts with the presence of noise.

## 2.4. NOVELTY OF PROPOSED DESIGN

The proposed design used as the entropy source in Figure 2.3 is the same as the Strong-Arm Latch circuit specified in Section 2.2.1. As it is not used as a dynamic comparator, its usage is different in order to convert it to a TRNG. In this structure, the offset is usually compensated by the feedback loop, which includes an analog circuit block connected to the control transistors.

The metastability-based TRNGs which have a fully digital design usually contain a cross-coupled inverter as in the Strong-Arm Latch. However, the control transistors are not included. For offset calibration, the cross-coupled inverter and the clock signal applied to the circuit are made tunable and controlled with a feedback loop containing a complex digital circuit block [14,15]. These types of design, which have been tested in 14-nm and 45-nm CMOS technologies before, may cause unacceptable limitations in terms of area occupation and power consumption in the older CMOS process. On the other hand, performance metrics such as throughput and energy efficiency are prone to be significantly reduced.

The novelty in the proposed design is to provide the offset calibration by changing the conductivity of the control transistors in the Strong-Arm latch circuit with a fully digital circuit block. The first advantage of this technique is that a high target entropy value is easily achieved with a sensitive conductivity change. Keeping the width of the control transistors larger and keeping the legs to be connected in parallel smaller offers high sensitivity for  $V_{step}$ . Another advantage is that even in the worst case in terms of process, voltage, and temperature variation, it can easily provide the offset compensation by offering manipulation

in the applied  $V_{CM}$  without sacrificing much entropy. Considering the disadvantage of the design, it requires a large number of parallel legs for offset compensation because the change in conductivity of the control transistors requires precision. Since the control of these legs is provided by a fully digital circuit, the maximum operating frequency is limited in the proposed design.



### 3. DESIGN STEPS

#### 3.1. DESIGN FLOW

The design starts with the TRNG core at first, and then the Self-Calibrating Loop subcircuit is designed. After adding the Correlation Suppressor subcircuit, it is more appropriate to design the Clock Delay circuit at last so that the entire circuit can work properly. During the design process, required analyzes should be tested on different PVT corners to ensure that the TRNG can work under various conditions. After these stages, the layout of the circuit is drawn in order to extract the parasitics. Lastly, the entire circuit is checked whether it works properly. If the design does not meet the targets, necessary arrangements should be made.

Before starting the design of the TRNG core, observing the effects of sizing the transistors in it provides an easier design process. The parameters  $\sigma_n$  and  $V_{step}$  are influential to reach the target entropy value determined in the design. Moreover, the  $V_{off}$  parameter represents the maximum offset that may occur in the circuit. To make a proper design, the TRNG core should operate as noisily as possible, step voltage should be chosen appropriately to meet the target entropy value, and an offset value should be set as smaller as possible. On the other hand, since the throughput of TRNG is also important, a clock frequency as high as possible should be given. Apart from all these effects, the power consumption of the TRNG core circuit should also be considered. Therefore, the first step of TRNG core design emerges to measure the effect of device sizing on noise, offset, step voltage, operating speed, and power consumption. Table 3.1 demonstrates the effects that are observed by increasing the channel widths of the transistors belonging to the proposed TRNG core circuit, which was given in Figure 2.3 in the previous chapter. Here, “+ + +” sign represents that the effect has increased significantly, “+” sign represents that the effect has increased, “0” represents that no significant effect is observed, “-” sign represents that the effect has decreased, and “- - -” sign represents that the effect has decreased significantly.

Table 3.1. Measured effects with increasing channel widths of devices in TRNG core

| Increase in Transistor Channel Width (W) | RMS Noise ( $\sigma_n$ ) | Offset Voltage ( $V_{off}$ ) | Step Voltage ( $V_{step}$ ) | Speed of Reset Phase | Speed of Evaluation Phase | Power Consumption |
|------------------------------------------|--------------------------|------------------------------|-----------------------------|----------------------|---------------------------|-------------------|
| $W_{S1,S2}$                              | — — —                    | —                            | + + +                       | +                    | 0                         | +                 |
| $W_{S3,S4}$                              | 0                        | 0                            | 0                           | + + +                | 0                         | + + +             |
| $W_{1-4}$                                | — — —                    | — — —                        | —                           | —                    | 0                         | +                 |
| $W_{5,6}$                                | 0                        | —                            | — — —                       | —                    | 0                         | +                 |
| $W_7$                                    | +                        | 0                            | 0                           | 0                    | + + +                     | +                 |

The conclusions to be deduced from Table 3.1 are as follows:

- Keeping the size of  $M_{S1,S2}$  precharge transistors smaller has a positive effect on both high  $\sigma_n$  value and low  $V_{step}$  value. However, since the offset voltage is negatively affected, reducing the width of these transistors should be done sufficiently.
- Keeping the size of  $M_{S3,S4}$  precharge transistors larger allows the reset phase to end faster. On the other hand, since power consumption is affected negatively, the width of these transistors should be increased sufficiently.
- Keeping the size of the cross-coupled inverter consisting of  $M_{1-4}$  smaller is beneficial in terms of RMS noise. However, it has a significant negative effect on offset voltage. Therefore, it is very important to reduce the dimensions until getting a tolerable  $V_{off}$  value.
- Keeping the size of  $M_{5-6}$  control transistors larger is suitable for achieving a small  $V_{step}$  value.
- Keeping the size of  $M_7$  larger provides a faster evaluation phase. However, this enlargement should be done carefully as it may adversely affect the  $\sigma_n$  and power consumption.

Apart from sizing, the effect of common-mode voltage on  $\sigma_n$  and  $V_{step}$  plays an important role. Decreasing  $V_{CM}$  lowers  $\sigma_n$  and rises  $V_{step}$  in a significant way. Therefore, applying a

maximum value of  $V_{CM}$ , which belongs to the  $V_{DD}$  level, is a suitable choice to obtain a maximum entropy value. Another case to consider is when the entropy value is above the target value, but the offset compensation is inadequate. In such a situation, decreasing  $V_{CM}$  a little so that it does not cause the entropy value to fall below the target, increases  $V_{step}$  and facilitates the offset compensation.

To begin with the TRNG core design, the effects in Table 3.1 should be considered and all necessary analyzes should be performed at different PVT corners. Thus, reference initial values are created for the TRNG core design, which is the first step of the design. The second step is to set an entropy target for the worst case. In the third step,  $W_{S1,S2}$  and  $W_{1-4}$  values are adjusted according to  $\sigma_n$  values. In the fourth step,  $V_{off}$  is measured. If the offset value is more than expected, it is returned to the third step. The fifth step is to obtain a target  $V_{step}$  parameter from the measured  $\sigma_n$  by the target entropy value. This aimed  $V_{step}$  value is reached by changing  $W_{5-6}$ . The sixth step is to measure  $\sigma_n$  and  $V_{off}$  values again. In the seventh step, the new  $\sigma_n$  and the new  $V_{step}$  values are compared to observe if the target entropy value is met. If the attained entropy is below the target, it is returned to the fifth step. In the eighth step,  $W_7$  is adjusted according to the power consumption and the duration of the evaluation phase. In the ninth step,  $\sigma_n$ ,  $V_{off}$ , and  $V_{step}$  are measured again. If the entropy value obtained after the measurements is not suitable, it should be returned to the third step of the design. In the 10th step, the size of the SCL subcircuit is determined according to the ratio of  $V_{off}$  and  $V_{step}$  values. In the 11th step, a clock period suitable for the TRNG core is determined. In the 12th step,  $W_{S3,S4}$  are adjusted in accordance with the duration of the reset phase. After the SCL subcircuit is designed, the  $V_{step}$  parameter may change. Considering that the  $\sigma_n$  value remains approximately the same, it causes a change in the entropy value of TRNG due to a different step voltage. Also, the size of the SCL to be designed may vary, as offset compensation is progressed by the ratio of  $V_{off}$  and  $V_{step}$ . For this reason, the 13th step is to decide whether the size of the SCL subcircuit is sufficient for the offset compensation. If the size is insufficient, it is returned to the 10th step. In the 14th step, using the designed SCL subcircuit,  $V_{step}$  is measured again with an extended measurement test setup and a new entropy calculation is made. If the entropy value is less than the target value, it is returned to the third step of the design. In the 15th step, the Correlation Suppressor subcircuit is designed. In the 16th step, the Clock Delay Circuits that will create the clock signal of the SCL and Correlation Suppressor structures are designed. Eventually, the electrical schematic

of the entire circuit is created. In the 17th step, the layout of the circuit is drawn and the parasitics of the entire circuit are extracted. In the last step, post-layout simulations are made on different PVT corners and it is checked whether the circuit works properly with the applied clock signals. If the clock signals are not suitable, going back to the 16th step is required. The flowchart diagram representing all these design steps is shown in Figure 3.1.



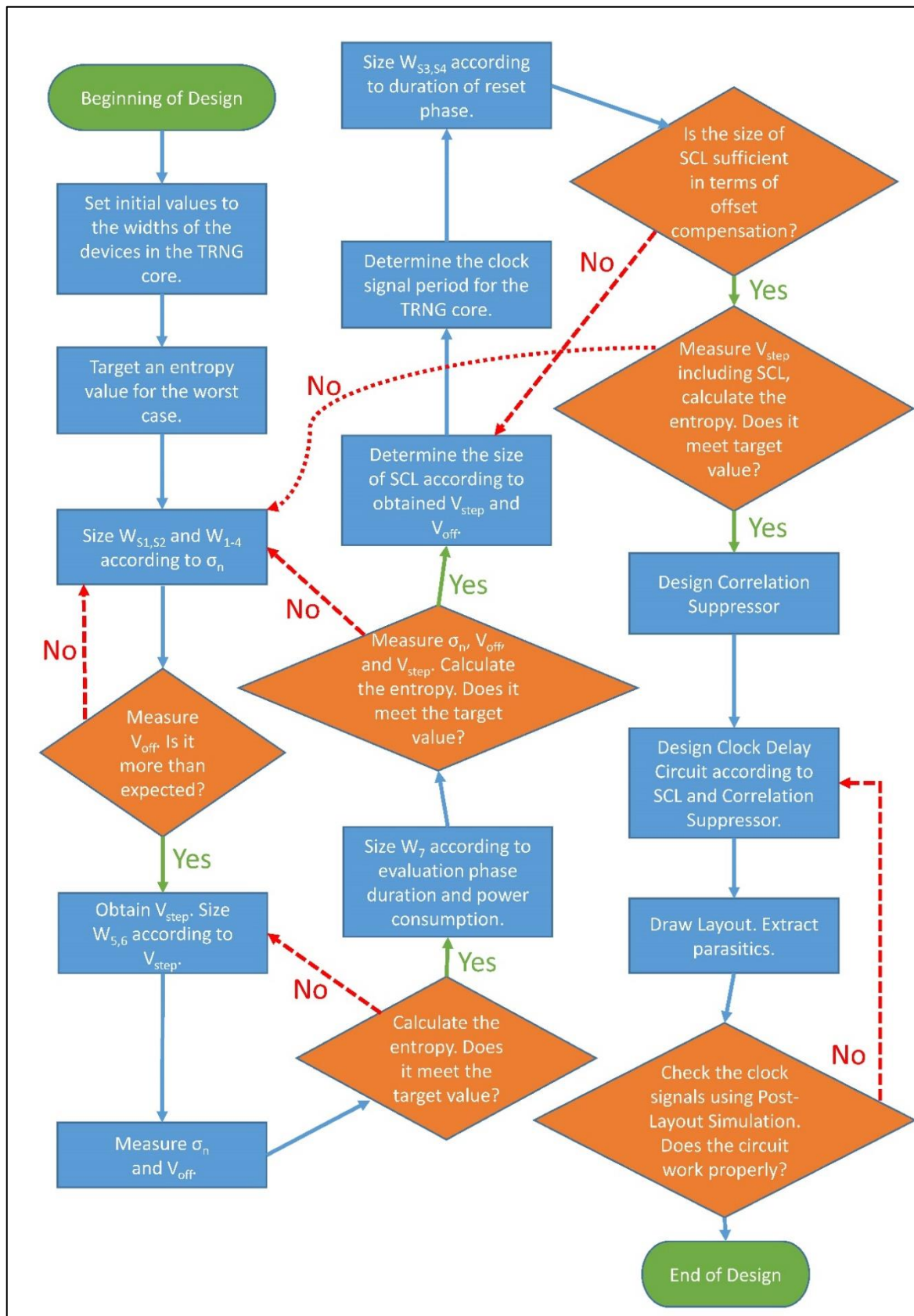


Figure 3.1. Flowchart diagram of entire circuit design



### 3.2.1. Periodic Noise Analysis

PAC analysis is used together with PSS/PNOISE analysis to find the effective value of the noise in the design. Figure 3.2 shows that a bias voltage of  $V_{CM}$  is applied to the inputs of the comparator. In order to apply a differential input voltage to the comparator, a dc voltage source named with  $V_N$  is connected between  $IA$  and  $V_{CM}$  nodes. This voltage source, which has a small DC amplitude, avoids circuit metastability in PSS/PNOISE analysis. In addition, this voltage source has a non-zero PAC magnitude which allows the PAC gain to be measured after PAC analysis.

PNOISE analysis calculates the average amount of noise power over a clock period. In dynamic comparators, noise is effective until the moment of decision. Since the presence of the noise in the circuit after the decision moment will not change the decision of the comparator, it is meaningless to measure the noise RMS value after this point. For this reason, an observation time represented with  $t_{obs}$  must be specified to measure the noise up to the desired point. After PSS analysis, which provides the periodic steady-state operating point calculation in the circuit, the  $t_{obs}$  value can be determined for later use in PNOISE and PAC analyzes. PNOISE analysis has several measuring options that are, time-domain noise (tdnoise) and phase modulation jitter (pmjitter). When using the tdnoise option, the value of the noise power at any time can be measured. Although the pmjitter option is used to calculate jitter, it can show output noise results like the tdnoise option. This option provides the noise power to be measured at a given trigger signal until it reaches a specified threshold level. The trigger signal here is the differential output voltage, and the threshold level is half of the  $V_{DD}$ , which is a suitable value for the decision moment. Therefore, it is convenient to measure the noise until the difference between the comparator outputs reaches half of the supply voltage.

The steps for measuring the RMS noise value using periodic noise analysis are as follows [20]:

- PSS analysis is created. “Shooting Engine” is selected as the analysis method. The clock signal that appears in the “Fundamental Tones” section is selected. The value of the “Beat Period” represented with  $T_b$ , should be chosen equally with the value of  $T$ , which is the period of the applied clock signal. When the “Beat Frequency” option

is selected instead of “Beat Period”,  $1/T_b$  value is assigned, or the “Auto Calculate” option can be used. A value of “10” is appropriate for the number of harmonics in the “Output Harmonics” section. In the “Accuracy Defaults” section, “conservative” is selected to obtain high accuracy results. In the “Transient-Aided Options” section, “Yes” or “Decide Automatically” is selected. If “Yes” is selected, the “Detect Steady State” option is automatically enabled. It also provides the possibility to enter the “tstab” parameter representing the time interval value. When this part is left blank, PSS simulation will be performed before the tstab simulation ends. The same can be done by selecting the “Decide Automatically” option in the “Transient-Aided Options” section.

- PSS simulation is run. After the simulation finishes, the differential output voltage is plotted from the PSS results and a  $t_{obs}$  value is determined. For this value, it is convenient to choose the assumed decision moment when the differential output voltage of the comparator reaches the level of  $V_{DD}/2$ .
- PNOISE analysis is created. In the “Output Frequency Sweep Range” section, 1 Hz and  $1/(2 \times T_b)$  Hz which is the Nyquist frequency are assigned as start and stop parameters, respectively. For high accuracy, “fullspectrum” is selected in the “Sidebands” section and a value of “10” is suitable for the maximum sideband value. Since the input-referred noise will be measured, the “Noise Figure” option is enabled. In the “Output” section, the voltage option is selected. After that, *OA* and *OB* nodes are marked from the circuit diagram as positive and negative output nodes. In the “Input Source” section, the voltage option is selected again and the  $V_N$  source is selected as the input voltage source. In the “Noise Type” section, the “jitter” option is selected. Finally,  $V_{DD}/2$  is assigned for the threshold value and the “rise” option is selected as crossing direction.
- PAC analysis is created. Relative is selected as “Sweep type” and relative harmonic value is assigned as “0”. In the “Input Frequency Sweep Range” section, 1 Hz and 50 GHz values are assigned as start and stop parameters, respectively. “Sweep Type” section can be left as “Automatic”. In the “Sidebands” section, the “maximum sideband” option is selected and the “0” value is assigned. In the “Specialized Analyzes” section, the “sampled” option is selected. Here, the voltage is selected as a signal and then, *OB* and *OA* nodes are marked from the circuit diagram as the positive and negative nets. As in the PNOISE analysis,  $V_{DD}/2$  is assigned as the

threshold value and the “rise” option is selected as the crossing direction. Finally, the “Maximum Samples” section is filled with the “1” value.

- PNOISE and PAC simulations are run together. After the simulations finish, the Total Output Noise spectrum is drawn from the tdnoise results section. The plot of noise power spectral density, represented with PSD, is obtained according to the  $t_{obs}$  value determined before. Here, the magnitude of the noise is determined as  $V^2/Hz$ . Since stop frequency  $1/(2 \times T_b)$  is selected in the PNOISE analysis, the resulting PSD graph is single-sided PSD. To find the average value of the noise power of the output, the entire PSD graph is integrated. Then, by taking the square root of the obtained value, the RMS noise value of the output, represented with  $\sigma_{n,o}$ , is obtained. The process for obtaining the  $\sigma_{n,o(t_{obs})}$  parameter according to a determined  $t_{obs}$  value is shown in Equation 3.1. Another more practical way to get the  $\sigma_{n,o}$  value is to select the “Integ Output Noise” function from the tdnoise results section. Here, the start and stop frequency values of 1 Hz and  $1/(2 \times T_b)$  Hz are typed manually. Therefore, it is possible to observe the same result obtained in Equation 3.1 when the magnitude value of the “Total Noise” value is set to “V”.

$$\sigma_{n,o(t_{obs})} = \sqrt{\int_0^{1/2T_b} PSD(f, t_{obs}) df} \quad (3.1)$$

- PAC results are opened. “Voltage Gain” is selected as a function and the “Differential Input and Output Nets” option is selected. In the “Sweep” and “Modifier” sections “spectrum” and “magnitude” options are selected, respectively. In the “Variable Value (eventtime)” section, the numeric value which appears below the time-averaged value is selected. This time value is calculated automatically according to the selected  $t_{obs}$  value by the simulation. In the “Input Harmonic” section, the “0” value is selected. Finally, the gain graph is acquired by marking the differential output and input nets,  $OB$ ,  $OA$ ,  $IA$ , and  $VCM(IB)$  nodes, respectively, from the circuit diagram. The DC gain value is obtained from this graph.

- The final step to calculate the RMS value of the noise is to divide the output RMS noise value measured with PNOISE by the gain measured with PAC. The formula of noise calculation is given in Equation 3.2. Here,  $G$  and  $\sigma_{n,i}$  represent the voltage gain and the input-referred noise according to a determined  $t_{obs}$  value.

$$\sigma_{n,i(t_{obs})} = \frac{\sigma_{n,o(t_{obs})}}{G} \quad (3.2)$$

- All performed steps are repeated on different PVT corners.

The input-referred noise obtained from Equation 3.2 is accepted as  $\sigma_n$  to be used in the entropy calculation.

### 3.2.2. Transient Noise Analysis

Another way to analyze noise in a Dynamic Comparator structure is to perform a transient noise analysis. The steps of this analysis are easier than the periodic noise analysis. However, the simulation time can take thousands of times longer. Therefore, it is highly recommended to use periodic noise analysis when performing noise characterization. It is more appropriate to use transient noise analysis for verification purposes.

The thermal noise that is the dominant noise type in the comparator is considered as white noise and performs a Gaussian distribution with a mean close to zero. Therefore, in order to find the RMS value of the noise in the transient noise analysis, this distribution is obtained and the standard deviation is calculated. Using the test setup in Figure 3.2 is also suitable for this type of noise analysis. This time,  $V_N$  is used as an offset voltage source and its amplitude is swept between the positive and the negative values of a specified value. To determine an appropriate offset value, the  $\sigma_n$  value calculated as a result of periodic noise analysis can be taken into account. If the magnitude of the offset value to be given to the comparator is much higher than the expected RMS noise value, the noise may not have any effect on the output decision of the comparator.

The steps for measuring the RMS noise value using transient noise analysis are as follows:

- Transient analysis is created. The value of one clock period is assigned as the stop time. For high accuracy, the “conservative” option is selected in the “Accuracy Defaults” section. Then, the “Transient Noise” option is enabled. As the “Noise Fmax” value is increased in this section, the simulation time gets longer. Therefore, choosing a value that is at least 50 times larger than the clock period is appropriate both in terms of simulation time and appropriate noise bandwidth value. After that, the “Multiple Runs” option is enabled. When this is enabled, the simulation will be repeated many times on different noise seeds. It is appropriate to enter a large number in the order of thousands in the “Number of Runs” section. Performing a single period multiple run analysis instead of a single run transient analysis for a long period makes it easy to count the total bit-1 and bit-0 values produced at the comparator outputs as a result of the simulation. Lastly, in the “Noise Contribution” section, the “on” option is selected and all transistors in the circuit diagram are marked for the “Instance List”. Thus, the comparator operates as completely noisy during the simulation.
- The dc amplitude of the  $V_N$  offset voltage source is assigned as a variable. This value is swept in the positive and negative directions at equal intervals, including zero. Determining the offset points at large and appropriate intervals reduces the amount of error to be made in the calculation of  $\sigma_n$ . As suitable endpoints are determined, usually 20-40 points are sufficient.
- Transient noise simulation is run parametrically. After the simulations finish, the total bit-1 values produced for each given offset are counted in order to access the probabilities of bit-1 production. Finally, these probability values are fitted to a Cumulative Distribution Function curve using statistical methods. The RMS noise value is reached after the standard deviation of this fitted CDF curve is calculated.
- All performed steps are repeated on different PVT corners.

### 3.2.3. Verification of Noise Measurement

Although periodic noise simulation is much faster than transient noise simulation, it is more complicated to prepare the test setup for the transient analysis. It is recommended to compare

the periodic noise results with the transient noise results for verification. The reason is that errors may occur during the test setup phase of the periodic noise analysis.

PNOISE and PAC simulation results used for periodic noise analysis at three different PVT corners of a sized TRNG core circuit are given in Figure 3.3 as an example. In order to gather the  $\sigma_n$ , the output noise values obtained from the PNOISE results are divided by the gain values obtained from the PAC results. The DC amplitude value of the  $V_N$  voltage source used in the simulations is 2 mV, and the PAC magnitude value is 1 V.

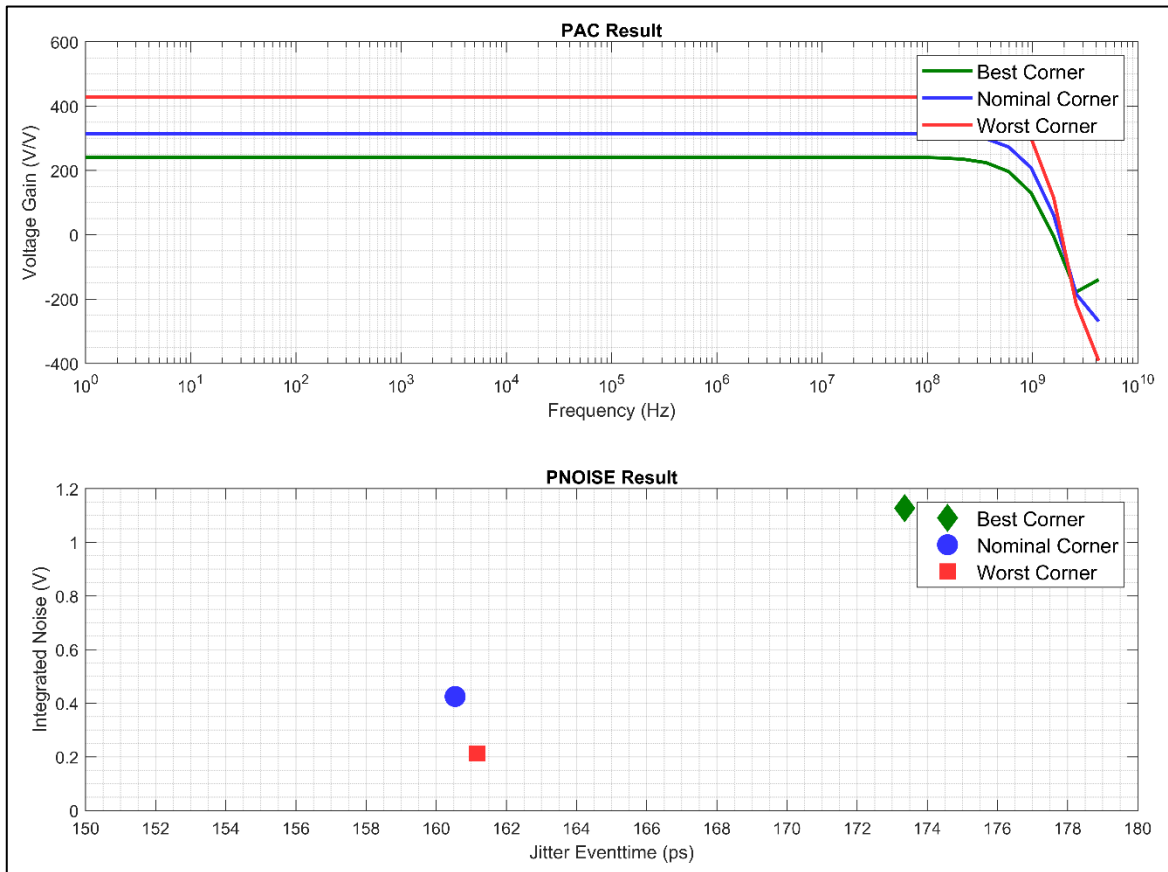


Figure 3.3. PAC and PNOISE simulation results

The values obtained from the transient noise analysis of the same circuit are available in Figure 3.4. In transient noise simulations, the DC amplitude value of the  $V_N$  voltage source is defined as a parametric variable changing between  $-2$  mV and  $2$  mV with  $100$   $\mu$ V intervals. Thus, there are 41 different measurement values for each corner. The probability

of bit-1 production is obtained as a result of the transient simulation using 5000 multiple runs within a clock period. The given offset values are marked as markers with different shapes and colors for each corner in Figure 3.4. According to these points, the CDF curves are fitted with a statistical approach and the standard deviation values of the Gaussian distributions are displayed at the bottom right on the figure.

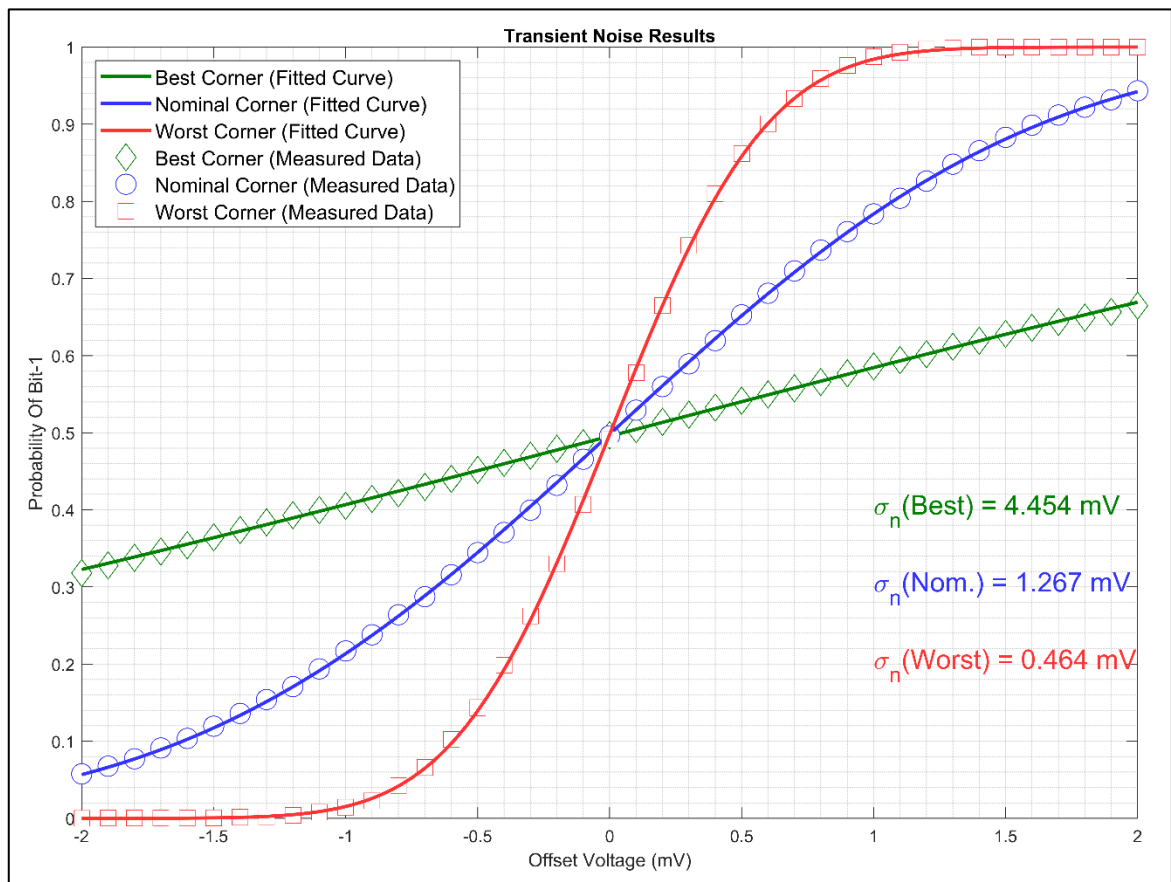


Figure 3.4. Transient noise simulation results

The RMS noise values measured after both types of noise analyzes and their comparison is shown in Table 3.2.

Table 3.2. Comparison of measured RMS noise results

| <b>Corner</b>  | <b><math>\sigma_n</math> from<br/>Periodic Noise<br/>Analysis</b> | <b><math>\sigma_n</math> from<br/>Transient Noise<br/>Analysis</b> | <b>Difference</b> |
|----------------|-------------------------------------------------------------------|--------------------------------------------------------------------|-------------------|
| Best Corner    | 4.667 mV                                                          | 4.454 mV                                                           | 4.8 %             |
| Nominal Corner | 1.353 mV                                                          | 1.267 mV                                                           | 6.8 %             |
| Worst Corner   | 0.497 mV                                                          | 0.464 mV                                                           | 7.1 %             |

### 3.3. MINIMUM ENTROPY CALCULATION

An important step in design is to set a target entropy value. This target value influences many steps of circuit design. Shannon Entropy calculation according to the probability of generated bit-1 and bit-0 is given in Equation 3.3. In this equation,  $p_1$  is the probability of bit-1, while the probability of bit-0 is expressed as  $1-p_1$  [22].

$$H(x) = -p_1 \log_2(p_1) - (1 - p_1) \log_2(1 - p_1) \quad (3.3)$$

As can be seen from the Shannon Entropy formula, in an ideal true random number generator where the entropy is equal to 1, the probability of generating bit-1 and bit-0 is 50 percent. In practice, this is not possible. The mean value of thermal noise, which is accepted as White Gaussian Noise, is zero and shows a distribution with a certain standard deviation. Even if an ideal noise occurs in the TRNG core where the additive and subtractive noise probabilities are exactly equal, there is an offset due to device mismatch in the circuit. While removing this offset, when enough steps are taken, the level at which the noise is effective is reached. After this level, forward or backward steps can be taken with the effect of noise. For this reason, to obtain a high entropy value, the steps taken in offset compensation must be smaller than the effective value of the noise.

Two important factors affecting the entropy in a metastability-based TRNG are the RMS value of the noise and the step voltage used to remove the offset. Based on these two values, the minimum entropy calculation can be found with a great approximation from Equation 3.4.  $H(x)$ ,  $\Phi$  indicated in the equation are Shannon Entropy and Cumulative Probability for Standard Normal Distribution function, respectively [23].

$$H(x) = -\log_2 [\Phi(V_{step}/2\sigma_n)] \quad (3.4)$$

The entropy value that occurs in the proposed design comes out with different results on different PVT corners. For this reason, an entropy value should be targeted for the worst case. Since TRNG goes through the post-processing operation at the end of the design, it is appropriate to target the worst-case entropy value to a minimum of 0.8.

### 3.4. STEP VOLTAGE MEASUREMENT

After the entropy calculation, a  $V_{step}$  value is formed that needs to be targeted. The offset compensation is provided by activating the legs connected in parallel to the control transistors in the proposed design one by one. Each step taken during this process creates a negative offset effect within the TRNG core. The value of this effect in terms of voltage is defined as the  $V_{step}$  parameter. When the offset compensation is significantly removed, it is entered into the band that where the noise is effective. Thus, random numbers begin to be generated in the TRNG. After this moment, the leg activation or deactivation process of both parts of TRNG starts to work opposite to each other. If the number of legs activated on any side is not minimum or maximum while generating random numbers, the  $V_{step}$  effect is doubled. Therefore, when measuring the  $V_{step}$  parameter for TRNG, a design should be made that gives at most half of the target  $V_{step}$  value obtained from the entropy calculation.

There are two different types of step voltage measurement processes in the design steps. In the first type,  $V_{step}$  is measured using only the TRNG core without designing the SCL circuit. In the second type, the  $V_{step}$  parameter is measured again after the SCL is designed. The reason is that the design structure of the NMOS Parallel Legs in the SCL subcircuit changes the  $V_{step}$  value measured in the first step.

The test setup for the first type of step voltage measurement is shown in Figure 3.5. The  $V_{step}$  measurement steps are as follows:

- A DC voltage source named  $V_{offA}$  is connected between the cross-coupled inverters in the TRNG core. Since this voltage source induces an offset effect into the right half part (part A) of the TRNG core, bit-0 is expected at OA output.
- An NMOS transistor is connected in parallel to the control transistor in the left half part (part B) of the TRNG core and  $V_{DD}$  is applied to its gate. On the other hand, this connected leg increases the offset effect on part B and tries to balance the given offset value in the part A.
- The DC amplitude of  $V_{offA}$  is parametrically changed to observe the bit-1 generation in the part A. Thus, the effect of one  $M_{leg}$  is measured in terms of the offset voltage. It is recommended to perform this operation using different numbers of legs. Although it is expected to measure n times the  $V_{step}$  value when n legs are used, this value may not comply exactly. As long as different numbers of legs are used, there may be upward or downward deviations in the expected  $V_{step}$  value. Hence, connecting as many parallel legs as possible and dividing the measured value by the number of legs used gives an appropriate average  $V_{step}$  value.
- All performed steps are repeated on different PVT corners.



- Two different types of clock signals are needed in the SCL subcircuit.  $V_{CLK2}$  pulse source is created for the clock input of the registers. All parameters of this pulse source except the delay time are the same as the  $V_{CLK}$  signal. The delay time to be given should be at least as long as the decision process in the evaluation phase of the TRNG ends and the outputs reach a stable state.
- $V_{CLK3}$  pulse source is created for the UDC clock inputs. This voltage source is similarly created by adding a delay to the  $V_{CLK2}$ . The delay time to be given should be at least as long as the Q output of the register is formed and remains stable for a certain amount of time.
- Initially, a pulse signal named with  $V_{CLR}$  is generated and given to the clear inputs of the UDCs to reset both of them. Similarly, the  $V_{CLR_N}$  pulse source which is the opposite of the  $V_{CLR}$  signal is created and applied to the clear inputs of the registers. Since there is no need to apply a preset signal to the registers,  $V_{DD}$  is given to the preset inputs of the registers.
- Since the UDC-B counts up to eliminate the given offset by  $V_{offA}$ , it is necessary to wait for the UDC-B to count up to the value that meets the offset compensation. If a large offset is given, the transient simulation takes too long due to the count operation of UDC-B. Instead, a preset signal can be applied to the UDC-B so that it can reach the maximum value at the desired time. To provide this process, a voltage source named  $V_{PRE}$  is created and given to the preset input of the UDC-B. As there is no need to preset the UDC-A, the preset input of this counter is connected to the ground.
- After all parameters are set for the test setup, the  $V_{step}$  value is measured by changing the DC amplitude of the  $V_{offA}$  parametrically as in the first type of  $V_{step}$  measurement. According to the number of steps taken, the  $V_{step}$  value can be easily measured by observing the occurrence of bit-1 in part A of the TRNG. Since it is possible to give a preset signal in this test setup, maximum offset compensation capability can also be calculated according to the designed SCL subcircuit size.
- All performed steps are repeated on different PVT corners.

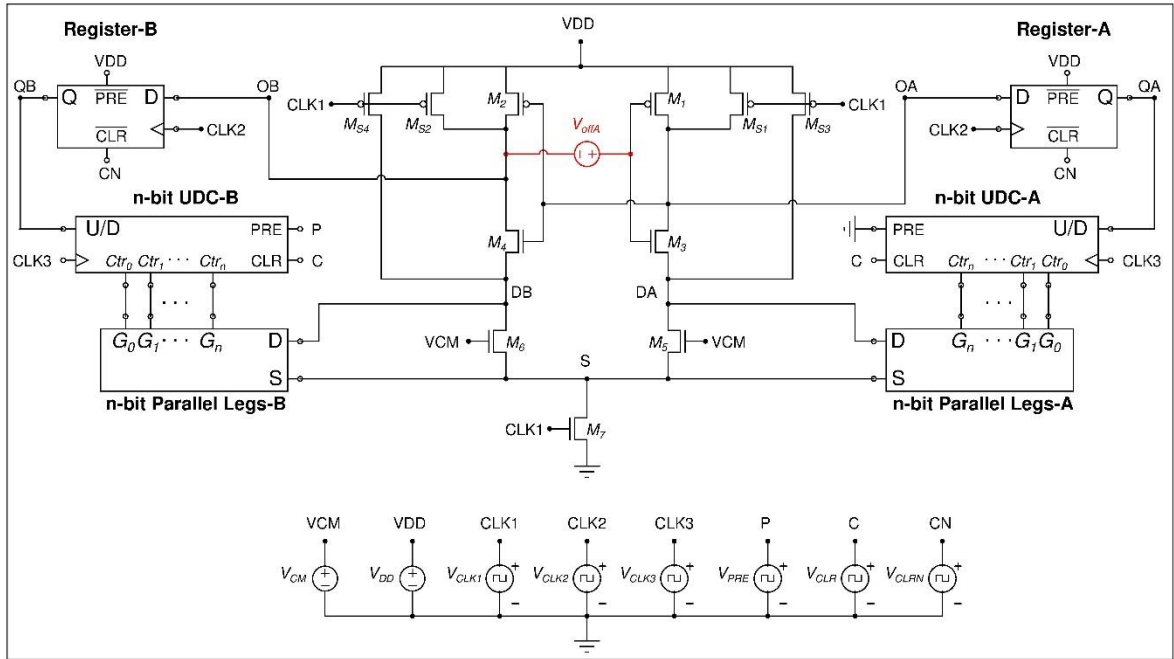


Figure 3.6. Test setup for the TRNG core step voltage measurement including SCL

### 3.5. OFFSET MEASUREMENT

In order to operate the TRNG core properly, the maximum offset value that may occur must be calculated and compensated. Offset measurement depends upon a two-stage test setup. The first setup requires a Monte Carlo analysis and then a transient simulation is needed.

The test setup of the first stage of the offset measurement is given in Figure 3.7. The steps for this stage are as follows:

- Two DC voltage sources named  $V_A$  and  $V_B$  are connected between the control transistors and the  $S$  node. Since these sources will be used to measure  $I_A$  and  $I_B$  branch currents, the DC amplitude values are assigned as 0 V.
- Transient analysis with a stop time that equals the clock period is created. In this analysis, the transient noise option must be disabled. The relevant Monte Carlo model library for the technology and devices used is selected. A variable named “sigma” having a value of “3” is assigned. An expression that calculates the maximum value of the magnitude of the current difference in both branches is

defined as an output setup. This calculated value represented with  $|I_{AB}|_{(\max)}$  is used for the next steps. The state of the analysis is saved.

- It is suitable to perform a Monte Carlo Sampling at  $3\sigma$  corners, as in the traditional Monte Carlo analysis. Thus, a Monte Carlo analysis is created and the saved state of the transient analysis is loaded.
- In the settings, “Process Data” and “Mismatch Data” options are enabled. It is appropriate to assign at least 1000 points for sampling. All the transistors are chosen from the circuit diagram after selecting the “Specify Instances/Devices” section.
- Various PVT corners are added in the “Corners” section and Monte Carlo analysis is started.
- After the simulation is completed, the “Yield” option is selected from the “Results” section. Here, the minimum and the maximum values of the output results are listed. The minimum value of the  $|I_{AB}|_{(\max)}$  on each PVT corner is recorded.

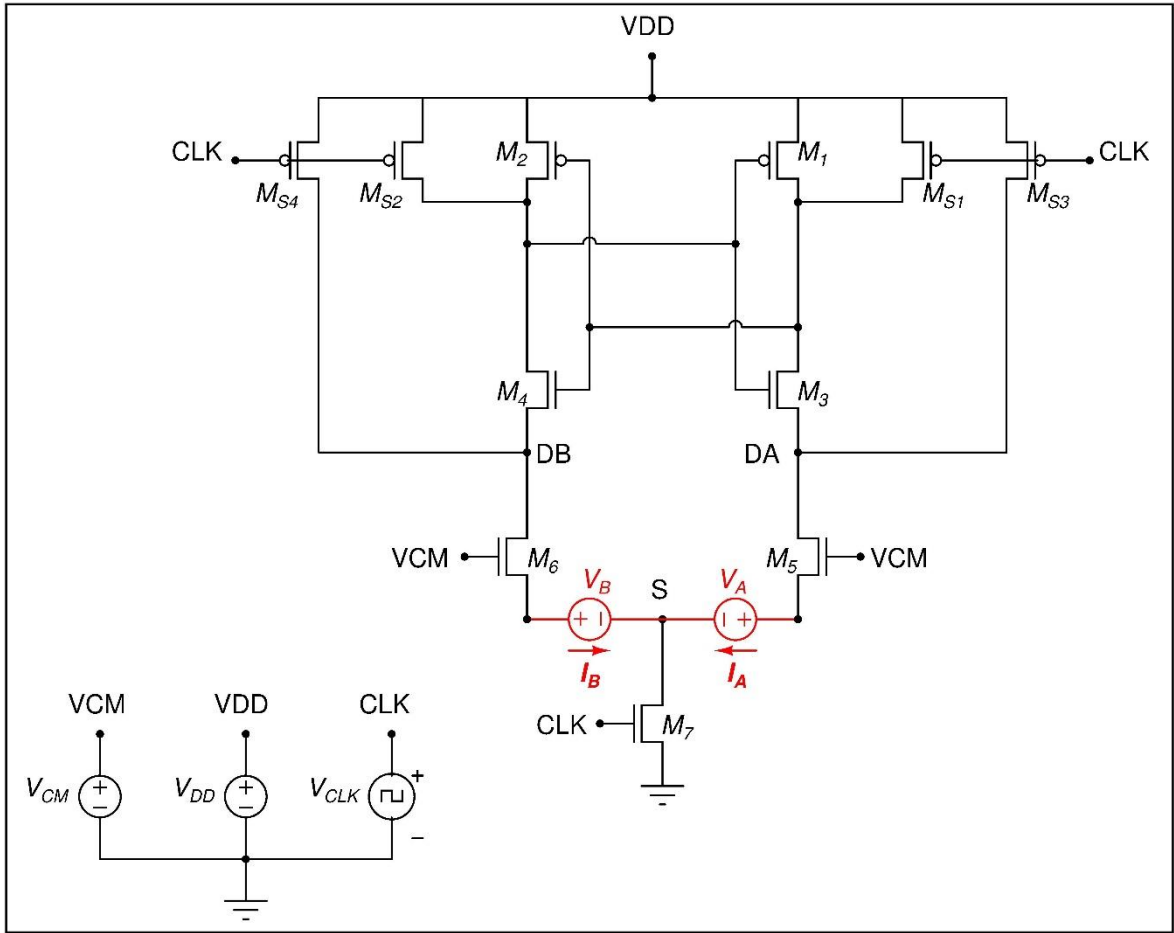


Figure 3.7. Test setup of the first stage for the TRNG core offset measurement

The test setup of the second stage of the offset measurement is given in Figure 3.8. The steps for this stage are as follows:

- As in the first stage of the offset measurement,  $V_A$  and  $V_B$  DC voltage sources for measuring  $I_A$  and  $I_B$  branch currents are added at the same place.
- A DC voltage source named  $V_{offA}$  is connected between the cross-coupled inverters as an offset voltage source. The DC amplitude value of this source is defined as a variable.
- Transient analysis with a stop time that equals the clock period is created. For the output setup, the  $|I_{AB}|_{(max)}$  expression used in the first offset measurement step is defined again. The transient noise option should be disabled. Transient analysis is performed by changing the DC amplitude value of the  $V_{offA}$ , parametrically.

- In the  $V_{offA}$  vs  $|I_{AB}|_{(max)}$  graphic obtained as a result of the simulations, it is determined which offset value corresponds to the minimum  $|I_{AB}|_{(max)}$  value measured in the first offset measurement stage. This value represents the  $V_{off}$  value of the TRNG core.
- All performed steps are repeated on different PVT corners.

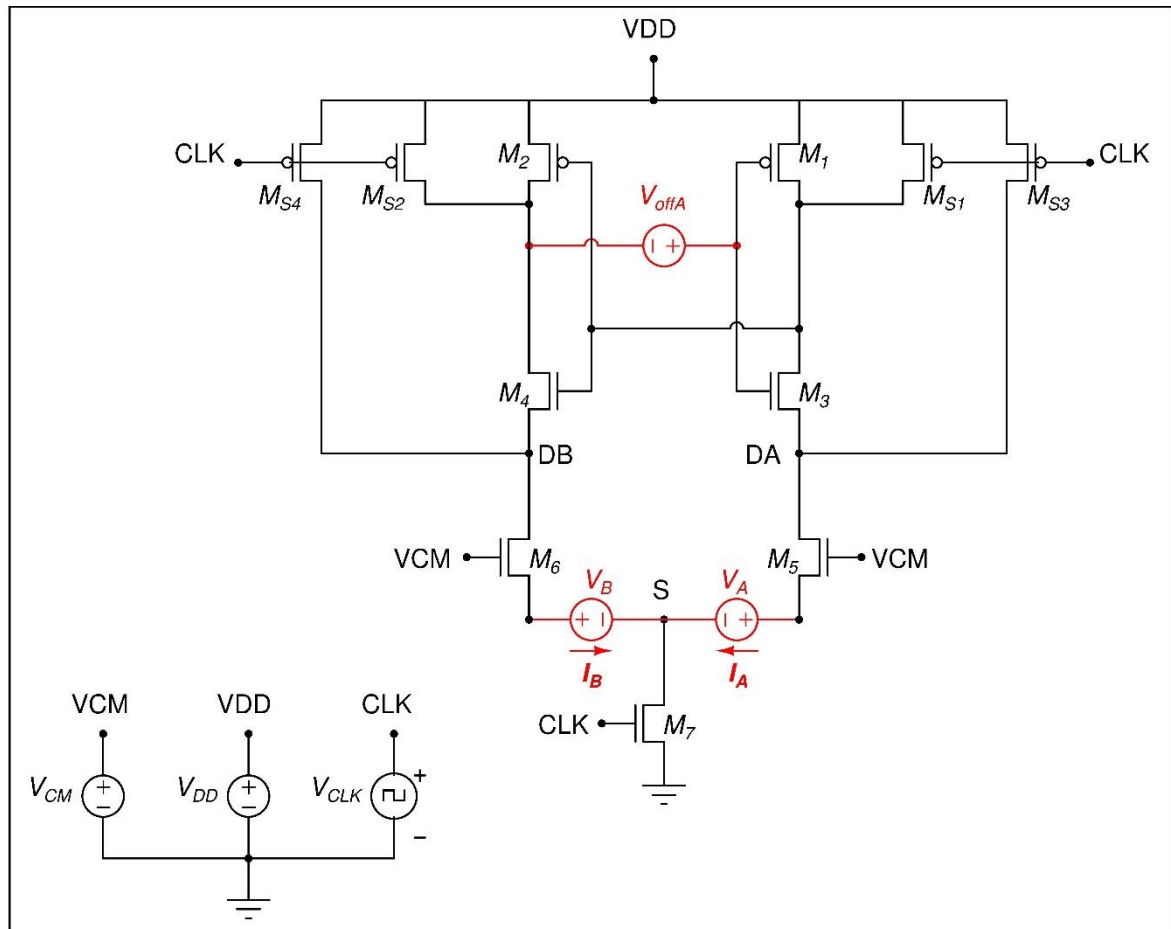


Figure 3.8. Test setup of the second stage for the TRNG core offset measurement

### 3.6. SIZE OF SELF-CALIBRATING LOOP

According to the  $V_{step}$  and  $V_{off}$  parameters measured in the design steps, the number of bits required for the UDC and NMOS Parallel Legs structures in the SCL subcircuit is decided. For the TRNG to generate random numbers, one of the UDC must count at least as much as the  $V_{off}/V_{step}$  ratio. Once the offset is significantly removed, the UDC may need to count

further due to the noise. Therefore, the bit number of the UDC is set above this calculated count value and adjusted to be the power of two. Increasing the UDC size by one bit causes the number of NMOS Parallel Legs to double. On the other hand, it requires an additional and larger staged buffer to the circuit. Increasing the SCL size not only increases the power consumption but also adds significant latency to the circuit. According to this situation, the minimum required frequency of the external clock signal should also be lowered. Therefore, it is critical to design the SCL size as small as possible in terms of power consumption, throughput, and footprint.

### 3.7. TIMING AND CLOCK DELAYS

It is not appropriate to use the externally applied main clock signal for TRNG core, symbolized with  $\phi_1$ , directly in subcircuits that need different clock signals in the entire circuit. In the evaluation phase, where  $\phi_1$  is high, a certain amount of time is required for the bits to be generated and become steady. Therefore, the register should wait at least this time to start sampling. The minimum delay time that should be given to the register clock signal, represented with  $t_{d(out1)}$ , is calculated according to Equation 3.5. The time elapsed from the beginning of the evaluation phase to the decision of outputs is  $t_{eval}$ . Furthermore,  $t_{su(reg)}$  is the setup time that the outputs should remain stable for a register.

$$t_{d(out1)} \geq t_{eval} + t_{su(reg)} \quad (3.5)$$

This newly acquired clock signal containing the phase difference as much as  $t_{d(out1)}$  appears as  $\phi_2$ . Since the registers are designed as rising edge-triggered, the time until the end of the sampling operation after the  $\phi_2$  reaches the rising edge consists of the propagation delay of a register. This period,  $t_{p(reg)}$ , should be shorter than the hold time of the register which will remain constant until the next change of the sampled inputs. Adjustment of this hold time,  $t_{h(reg)}$ , is given in Equation 3.6. Similarly, it is possible to apply  $\phi_2$  to the clock input of the Correlation Suppressor subcircuit, which contains registers in it. It is sufficient to add a bigger staged buffer to the one that will also drive the Correlation Suppressor subcircuit out of the two clock delay circuits.

$$t_{h(reg)} > t_{p(reg)} \quad (3.6)$$

On the other hand, the Up-Down Counter (UDC) does the counting forward or backward step according to the values sampled in the registers which are also up and down signals. Before starting UDC sampling, the  $U/D$  signal should have been formed, and accordingly, the toggle or hold signals of the JK Flip-Flops inside the UDC must be formed. Here, the propagation delays of the logic gates in the UDC,  $t_{p(gates)}$ , play a role.  $T_{0-10}$ , which are the input signals of the flip-flops (FFs), occur in the order. Since the voltage of the last node,  $T_{10}$  may change, this signal must be formed and remain stable for a certain amount of time. This setup time is represented with  $t_{su(fff)}$ . Moreover, the obtained new clock signal including a phase difference of  $t_{d(out2)}$  is represented with  $\phi_3$ .  $t_{d(out2)}$  is set according to Equation 3.7.

$$t_{d(out2)} \geq t_{d(out1)} + t_{p(reg)} + t_{p(gates)} + t_{su(fff)} \quad (3.7)$$

When the rising edge of  $\phi_3$  arrives, inputs of FFs are sampled to be toggled or held. This sampling process takes place during the high level of  $\phi_3$ . In order to use  $\phi_3$  efficiently, it is necessary to keep this high-level time as short as possible and give more to the low level. For the high-level duration of  $\phi_3$ , whose pulse width does not have to be half of a period, at least the master part of the FFs play role in terms of propagation delay. This delay time is represented with  $t_{p(fff)}$ . The pulse width of  $\phi_3$  which is  $\phi_{3H}$  should be more than  $t_{p(fff)}$  to complete sampling. Since  $\phi_{3H}$  is shorter than the hold time for FFs, it would be meaningless to calculate the hold time. Therefore, the calculation of  $\phi_{3H}$  is made from Equation 3.8.

$$\phi_{3H} > t_{p(fff)} \quad (3.8)$$

After the falling edge of  $\phi_3$  comes, UDC starts changing the output bits according to the counting operation. In this way, the gate terminals of NMOS parallel legs are charged or discharged via staged buffers driven by UDC. Fully charging or discharging the gate of a leg until the beginning of the next evaluation phase is important in terms of controlling the

conductance. The total time that FFs produce their outputs is originated from the propagation delay of its slave part. Also adding the delays of the staged buffers placed between these FFs and legs, the total delay is represented with  $t_{p(ffs)}$ . This value is selected according to Equation 3.9. In this equation,  $\phi_{3L}$  indicates the low level of  $\phi_3$ .

$$\phi_{3L} - t_{d(out2)} > t_{p(ffs)} \quad (3.9)$$

The resulting period of being modified  $\phi_2$  and  $\phi_3$  clock signals are identical to the period of  $\phi_1$ . The minimum value of this clock period,  $T$ , is determined by the delay calculations made in  $\phi_3$ . Equation 3.10 gives the minimum clock period that can be applied externally. When adjusting all the clock signals, different Process-Voltage-Temperature (PVT) corner effects and post-layout parasitic effects should also be considered to run the entire circuit under the worst condition.

$$T \geq \phi_{3H(min)} + \phi_{3L(min)} \quad (3.10)$$

In Figure 3.9, properly organized  $\phi_1$ ,  $\phi_2$ , and  $\phi_3$  signals are indicated. Here, the register outputs that sample  $V_{OA}$  and  $V_{OB}$  values are expressed as  $Q_A$  and  $Q_B$ . The  $T_{10}$  node, which has a critical value for  $\phi_3$ , represents the input of the FF-10 in the UDC.  $CtrA_0$  and  $CtrA_1$  stand for the first two bits of UDC counting from  $Q_A$ .

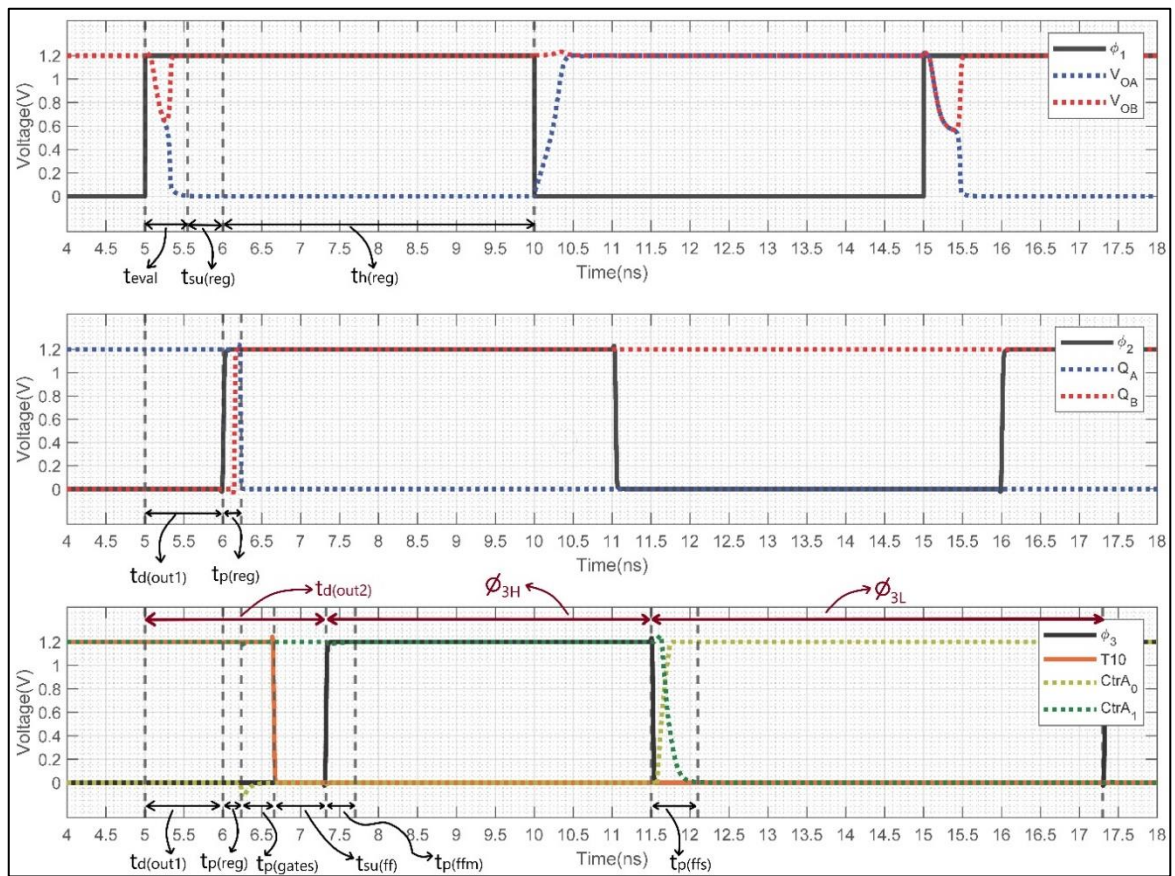


Figure 3.9. Clock timing diagrams

## 4. TRNG CIRCUIT DESIGN

### 4.1. TRNG CORE

The proposed TRNG core circuit was examined in Chapter 2. Using the design steps in Chapter 3, the widths of the transistors inside the circuit are determined. The sizing values used in the design are given in Table 4.1.

Table 4.1. Device sizes of TRNG core

| Device Name | Length | Finger Width    | Finger Number | Total Width       |
|-------------|--------|-----------------|---------------|-------------------|
| $M_{S1-S2}$ | 60 nm  | 1 $\mu\text{m}$ | 1             | 1 $\mu\text{m}$   |
| $M_{S3-S4}$ | 60 nm  | 5 $\mu\text{m}$ | 1             | 5 $\mu\text{m}$   |
| $M_{1-2}$   | 60 nm  | 5 $\mu\text{m}$ | 1             | 5 $\mu\text{m}$   |
| $M_{3-4}$   | 60 nm  | 5 $\mu\text{m}$ | 1             | 5 $\mu\text{m}$   |
| $M_{5-6}$   | 60 nm  | 5 $\mu\text{m}$ | 40            | 200 $\mu\text{m}$ |
| $M_7$       | 60 nm  | 5 $\mu\text{m}$ | 2             | 10 $\mu\text{m}$  |

### 4.2. LOGIC GATES

All logic gates in the entire circuit are designed with the basic static CMOS logic gate methodology except the XOR gate used in the Correlation Suppressor. In order to keep the high-to-low and low-to-high propagation delays of the logic gates,  $T_{PHL}$  and  $T_{PLH}$ , close to each other, PMOS/NMOS device width ratio is calculated according to the formulas given in Table 4.2. The terms  $J_{N(max)}$ ,  $J_{P(max)}$ , and  $n$  used in the equations represent NMOS saturation drive current, PMOS saturation drive current, and fan-in number of a logic gate, respectively. Since the ratio of saturation device currents may deviate slightly for different width values, a parametric dc operating point analysis can be performed to determine the average value of  $J_{N(max)}/J_{P(max)}$ . AND and OR gates are designed similar to NAND and NOR gates by adding only NOT gate at the front end.

Table 4.2. Device sizes of CMOS logic gates

| Logic Gate       | Width Ratio Equations                                         | Fan-in (n) | Length | PMOS Width         | NMOS Width |
|------------------|---------------------------------------------------------------|------------|--------|--------------------|------------|
| NOT              | $\frac{W_P}{W_N} = \frac{J_{N(max)}}{J_{P(max)}}$             | 1          | 60 nm  | 165 nm             | 80 nm      |
| 2-Input NAND/AND | $\frac{W_P}{W_N} = \frac{1}{n} \frac{J_{N(max)}}{J_{P(max)}}$ | 2          | 60 nm  | 85 nm              | 80 nm      |
| 2-Input NOR/OR   | $\frac{W_P}{W_N} = n \frac{J_{N(max)}}{J_{P(max)}}$           | 2          | 60 nm  | 335 nm             | 80 nm      |
| 3-Input NAND     | $\frac{W_P}{W_N} = \frac{1}{n} \frac{J_{N(max)}}{J_{P(max)}}$ | 3          | 60 nm  | 80 nm              | 115 nm     |
| 12-Input AND     | $\frac{W_P}{W_N} = \frac{1}{n} \frac{J_{N(max)}}{J_{P(max)}}$ | 12         | 60 nm  | 80 nm              | 460 nm     |
| 12-Input NOR     | $\frac{W_P}{W_N} = n \frac{J_{N(max)}}{J_{P(max)}}$           | 12         | 60 nm  | 2.01 $\mu\text{m}$ | 80 nm      |

### 4.3. STAGED BUFFERS

The staged buffer design is used to drive the large capacitances formed in the entire circuit faster. Some parameters must be taken into account in order to design the staged buffer consisting of an inverter chain in an optimum way.

As far as latency in the staged buffer is considered, PMOS/NMOS device width ratio in each inverter should be as in Equation 4.1. In this equation, the  $W_{P(i)}$  and  $W_{N(i)}$  values represent the PMOS width and the NMOS width at each stage, respectively.

$$\frac{W_{P(i)}}{W_{N(i)}} = \sqrt{\frac{J_{N(max)}}{J_{P(max)}}} \quad (4.1)$$

In Equation 4.2, another formula is given to be used for the calculation of the staged buffer parameters. Here  $C_{ox}$ ,  $\epsilon_{ox}$ , and  $TOX$  are the oxide capacitance per unit gate area, the dielectric constant of gate oxide, the thickness of gate oxide, respectively. The  $TOX$  value, which is a technology-dependent parameter, must be found from the PDK used.

$$C_{ox} = \frac{\epsilon_{ox}}{TOX} \quad (4.2)$$

The value of  $n$ , which determines how many stages the staged buffer should include, is calculated from Equation 4.3. The  $C_L$ ,  $L_{min}$ ,  $W_{N(1)}$ , and  $CGSO$  values in this equation represent the load capacitance, the possible minimum device length, the channel width of the NMOS transistor in the first stage, and the overlap capacitance per meter of channel width, respectively. It is convenient to choose the possible minimum device width of the used technology for the  $W_{N(1)}$ . The  $CGSO$  value, which is a technology-dependent parameter, must be found from the PDK used. After that, the average of the two different  $CGSO$  values corresponding to NMOS and PMOS is used in the formula.

$$n = \ln \left[ \frac{C_L}{\left( 1 + \sqrt{\frac{J_{N(max)}}{J_{P(max)}}} \right) (L_{min} C_{ox} + 2 \times CGSO) W_{N(1)}} \right] \quad (4.3)$$

The number  $n$  calculated from Equation 4.3 is floored to the closest integer number. For all staged buffers in the design to transmit the same incoming signal,  $n$  must be an even number. According to this rounded  $n$  value, the value of  $m$  which specifies how many times each stage should grow is calculated from Equation 4.4.

$$m = \left[ \frac{C_L}{\left( 1 + \sqrt{\frac{J_{N(max)}}{J_{P(max)}}} \right) (L_{min} C_{ox} + 2 \times CGSO) W_{N(1)}} \right]^{\frac{1}{n}} \quad (4.4)$$

According to the values obtained as a result of all calculations, the parameters of the staged buffers used in both parts of TRNG are shown in Table 4.3.

Table 4.3. Staged-buffers used for both parts of TRNG

| Location                               | Number of stages (n) | Tapering Factor (m) |
|----------------------------------------|----------------------|---------------------|
| UDC (Ctr0) – NMOS Parallel Legs (G0)   | 4                    | 3.3472              |
| UDC (Ctr1) – NMOS Parallel Legs (G1)   | 4                    | 3.3472              |
| UDC (Ctr2) – NMOS Parallel Legs (G2)   | 4                    | 3.3472              |
| UDC (Ctr3) – NMOS Parallel Legs (G3)   | 4                    | 3.3472              |
| UDC (Ctr4) – NMOS Parallel Legs (G4)   | 4                    | 3.4377              |
| UDC (Ctr5) – NMOS Parallel Legs (G5)   | 4                    | 3.4377              |
| UDC (Ctr6) – NMOS Parallel Legs (G6)   | 4                    | 3.4812              |
| UDC (Ctr7) – NMOS Parallel Legs (G7)   | 4                    | 3.5569              |
| UDC (Ctr8) – NMOS Parallel Legs (G8)   | 4                    | 3.7957              |
| UDC (Ctr9) – NMOS Parallel Legs (G9)   | 4                    | 4.0412              |
| UDC (Ctr10) – NMOS Parallel Legs (G10) | 6                    | 2.8569              |
| <i>PN</i> out in UDC (Buffer-1)        | 4                    | 3.4552              |
| <i>CN</i> out in UDC (Buffer-2)        | 4                    | 3.4552              |

Although the entire circuit is designed as symmetrically as possible, some staged-buffer designs have different values on the different sides of the TRNG. The reason is that the Correlation Suppressor structure is located only on one side of the TRNG. The parameters of the staged buffers used for different parts are given in Table 4.4.

Table 4.4. Staged-buffers used for different parts (Part A and Part B) of TRNG

| Location                                      | Number of stages (n) | Tapering Factor (m) |
|-----------------------------------------------|----------------------|---------------------|
| Register(A) – UDC(A) & Correlation Suppressor | 4                    | 3.2396              |
| Register(B) – UDC(B)                          | 4                    | 3.2396              |
| CLK <sub>OUT1</sub> in Clock Delay Circuit(A) | 4                    | 3.9552              |
| CLK <sub>OUT2</sub> in Clock Delay Circuit(A) | 4                    | 3.5765              |
| CLK <sub>OUT1</sub> in Clock Delay Circuit(B) | 4                    | 3.2317              |
| CLK <sub>OUT2</sub> in Clock Delay Circuit(B) | 4                    | 3.5765              |

#### 4.4. FLIP-FLOPS

Two types of static flip-flop structures are used in the design. The first type, D-Type Flip-Flop (Register), is used to sample the TRNG core output and to create blocks in the Correlation Suppressor structure. The second type, JK Flip-Flop, is used to create the UDC subcircuits. Both flip-flops are designed in master-slave structure in order to continue to function for a full clock period.

##### 4.4.1. D-Type Flip-Flop (Register)

It is more appropriate to make a positive edge-triggered D-Type Flip-Flop since bits are produced in the TRNG core after the evaluation phase starts on the rising edge of the clock. In this way, the register can be operated by applying a similar clock signal to the main clock signal of the TRNG core, and the outputs can be sampled for a full clock period. This structure whose logic diagram is shown in Figure 4.1 consists of six NAND gates and also has preset and clear features. To activate preset and clear operation, logic-0 signal should be applied to  $\overline{PRE}$  and  $\overline{CLR}$  inputs, individually. The truth table of this structure is presented in Table .5. While the up and down arrow signs in the table stand for the rising and falling edge of the clock signal, the letter “X” represents the “Don’t Care” state.

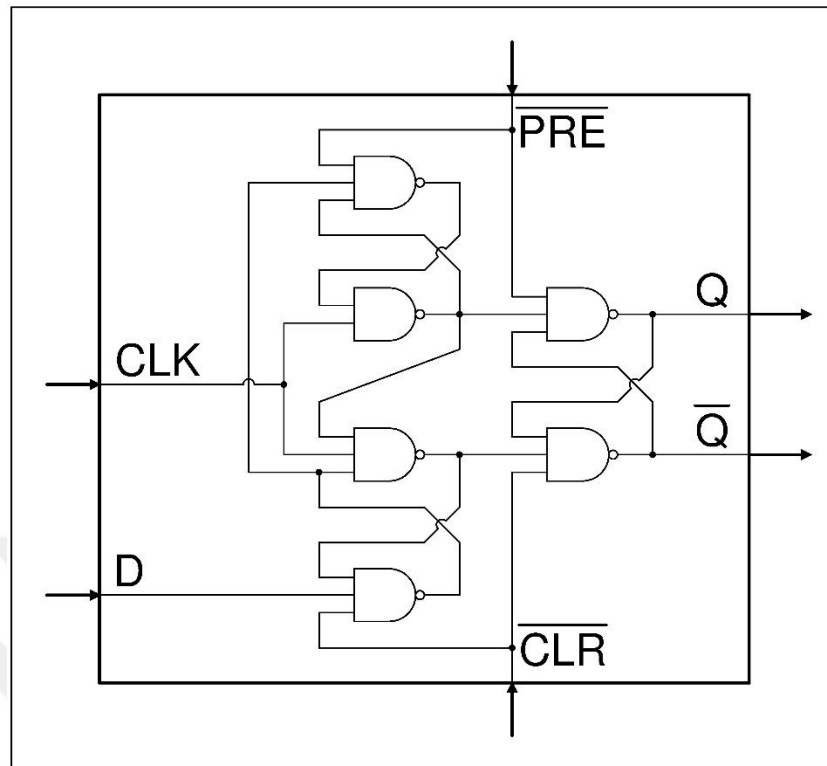


Figure 4.1. Rising edge triggered D-Type Flip-Flop (Register) with preset and clear inputs

Table 4.5. Truth table of rising edge triggered D-Type Flip-Flop with preset and clear inputs

| CLK | D | $\overline{\text{CLR}}$ | $\overline{\text{PRE}}$ | Q | $\bar{Q}$ |
|-----|---|-------------------------|-------------------------|---|-----------|
| ↑   | 0 | 1                       | 1                       | 0 | 1         |
| ↑   | 1 | 1                       | 1                       | 1 | 0         |
| ↓   | X | 1                       | 1                       | Q | $\bar{Q}$ |
| X   | X | 0                       | 1                       | 0 | 1         |
| X   | X | 1                       | 0                       | 1 | 0         |
| X   | X | 0                       | 0                       | 1 | 1         |

#### 4.4.2. JK Flip-Flop

For the purpose of building a conventional Up-Down Counter, T Flip-Flops are required for each count of bits. To provide this function, J and K inputs are connected in each JK Flip-Flops. As in the register design, it is more convenient to design the JK Flip-Flop (JKFF) in the form of master-slave and positive edge-triggered. If the JK input sampled on the rising edge of the clock is logic-0, the output value is held on the falling edge of the clock. Otherwise, if the JK input sampled on the rising edge of the clock is logic-1, the output is toggled on the falling edge of the clock. Herewith, the output values are stored for a period from the falling edge of the clock to the falling edge. Furthermore, it is possible to use a similar clock signal in this flip-flop as in the TRNG core and register. The JKFF design consisting of eight NAND gates and one NOT gate is shown in Figure 4.2. Like in the register, JKFF also includes preset and clear inputs activated by the logic-0 signal. The truth table for this structure is given in Table 4.6.

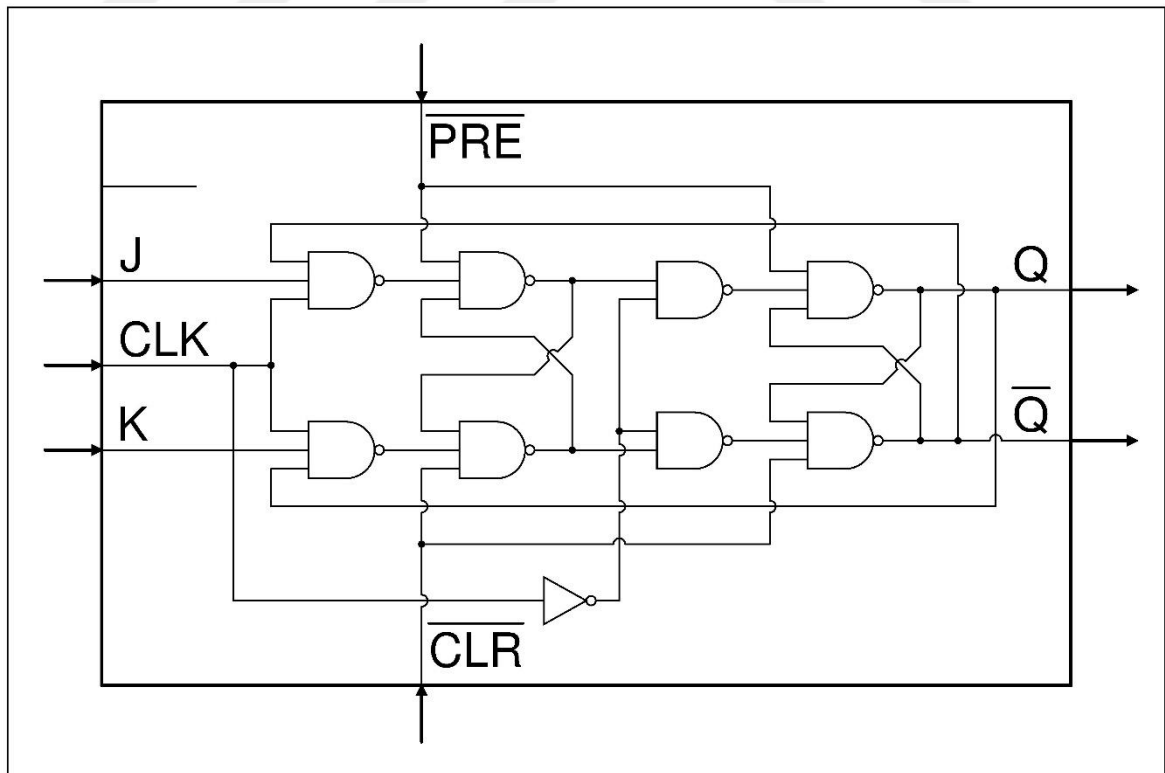


Figure 4.2. Positive edge triggered Master-Slave JK Flip-Flop with preset and clear inputs

Table 4.6. Truth table of positive edge triggered Master-Slave JK Flip-Flop with preset and clear inputs

| CLK | JK | $\overline{\text{CLR}}$ | $\overline{\text{PRE}}$ | Q                                        | $\overline{\text{Q}}$ |
|-----|----|-------------------------|-------------------------|------------------------------------------|-----------------------|
| ↑   | 0  | 1                       | 1                       | Q                                        | $\overline{\text{Q}}$ |
| ↑   | 1  | 1                       | 1                       | Q                                        | $\overline{\text{Q}}$ |
| ↓   | X  | 1                       | 1                       | HOLD if JK=0 at ↑<br>TOGGLE if JK=1 at ↑ |                       |
| X   | X  | 0                       | 1                       | 0                                        | 1                     |
| X   | X  | 1                       | 0                       | 1                                        | 0                     |
| X   | X  | 0                       | 0                       | 1                                        | 1                     |

#### 4.5. SELF-CALIBRATING LOOP

As a result of the design steps in Chapter 3, it was decided that the Self-Calibrating Loop subcircuit should be designed as 11 bits. Thus, SCL consists of an 11-Bit Custom Up-Down Counter and 11-Bit NMOS Parallel Legs including a total number of  $2^{11}-1$  transistors. The register in SCL takes place as mentioned in Section 4.4.1.

The register samples one of the output bits generated by the entropy source and transfers it to the UDC. According to being this output bit-1 or bit-0, the counter counts upward or downward and turns one leg on or off.

##### 4.5.1. Custom Up-Down Counter

A custom Up-Down Counter design is needed in the SCL subcircuit. When a conventional counter counts up after reaching the maximum number, it resets itself. Likewise, in a countdown operation when the counter value is zero, the counter sets all its bits to logic-1 and reaches the maximum count value. Since the NMOS legs should be opened and closed one by one during the offset compensation, it becomes impossible to control this situation with a standard UDC design.

It is recommended to initially reset the UDC values together with the registers in the entire circuit when TRNG starts to operate. In the next period after initializing operation, bit-1 and bit-0 are produced by TRNG and the values are sampled by registers. Hence, one of the UDC counts up and the other counts down. UDC that wants to count down from zero must be locked at zero value in order not to increase to the maximum value. On the other hand, TRNG still continues to generate numbers with the presence of noise even if UDC does not reach its maximum value after offset compensation is complete. Thus, the UDC value continues to change after offset compensation ends. Therefore, the possibility of one of the UDC count values reaching the maximum should also be considered. If it needs to count up again after reaching the maximum, it must be locked at the maximum value so that it does not reset itself. One way to achieve this goal is to send a common preset signal to the JK flip-flops inside the UDC. Likewise, if the UDC value is at the minimum and there is a signal to count down, a common reset signal should be sent. Accordingly, the flip-flops are designed with a common preset and clear input as shown in Figure 4.3. Nodes *PN* and *CN* represent the common preset and clear inputs of flip-flops, respectively.

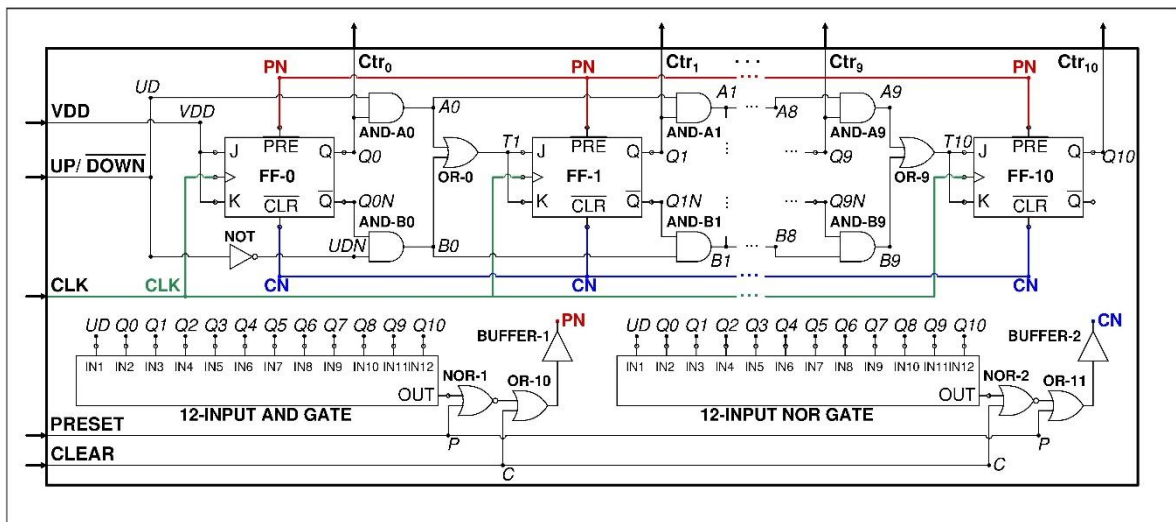


Figure 4.3. 11-Bit Custom Up-Down Counter with preset and clear inputs

The condition in which UDC wants to count up after reaching its maximum is the case where the UDC output bits,  $Q_{0-10}$ , and the  $UP/\overline{DOWN}$  signal,  $UD$ , are at logic-1. In this case, it is necessary to make  $PN = 0$  to keep the UDC at the maximum number. The logic gate that

allows the output to be logic-1 while only all inputs are logic-1 is a 12-Input AND gate. Since the preset or clear inputs of JK Flip-Flops are activated with binary-low, the output of the 12-Input And gate is passed through the NOR-1 gate. Regardless of the other input of this NOR-1 gate, when the output of the 12-Input AND gate is at logic-1, the output of the NOR-1 gate will be logic-0. Therefore, a logic-0 signal is sent to the common preset input of the flip-flops and UDC automatically presets itself. The second input of the NOR-1 gate provides the opportunity to give an external preset input to the UDC. When logic-1 is given to this input from the outside, the NOR-1 gate generates a logic-0 signal independently from the first input and presets the UDC. In fact, all these conditions mentioned are valid only when the second input of the OR-10 gate, which is also driven by the NOR-1 gate, is at logic-0. The purpose of this gate is to prevent the  $PN = 0$  condition when a clear input is given externally to the UDC which is in preset condition. In consideration of both  $PN$  and  $CN$  nodes are binary low, the FFs cannot be reset.

Similarly, in the situation in which UDC wants to count down when its value is at minimum, clearing the FFs is achieved by controlling the  $CN$  node instead of  $PN$ . Considering the same logic, a 12-input AND gate is replaced with a 12-input NOR gate. This time,  $C$  and  $P$  nodes are connected to the other inputs of NOR-2 and OR-11 gates, respectively.

Since it is determined that the size of the UDC should be 11-bit by the SCL design, 11 JKFFs are needed. As the least significant bit always changes during counting upward or downward, FF-0 must toggle continuously. To ensure this situation, the JK input of FF-0 is connected to  $V_{DD}$ . With the  $UD$  signal, the outputs of the FFs pass through the logic gates and allow other FFs to toggle or hold.

One of the important issues to be considered in the design is the maximum propagation delay calculations that can occur in this UDC. The clock frequency to be given to the UDC must meet these delays and the charging or discharging process of the relevant NMOS Parallel Legs must be completed before the evaluation phase of the TRNG core circuit starts. The custom UDC consisting of JKFFs with a synchronous structure is controlled by a clock signal. When the clock level is high, which of the FFs should be held or toggled is determined. The node that may change during this operation lastly is the  $T10$  node, which is the input of FF-10. The total delay of 10 AND-A or 10 AND-B gates connected in serial with OR-10 gate plays an important role in the maximum propagation delay calculation here. When the clock signal falls, the synchronous FFs which are in toggle mode start to change

their outputs at the same time. However, since each of them drives the gate terminal of a different number of NMOS Parallel Legs, different load capacitance values occur at their outputs. With the help of staged buffers designed in accordance with the capacitance values at outputs, these durations can be brought closer to each other. As a result, in the calculation of the maximum propagation delay on the low level of the clock, the total delay of one FF and the buffer driven by it should be taken into account.

#### 4.5.2. NMOS Parallel Legs

NMOS Parallel Legs which form another part of the SCL subcircuit, are designed according to the number of bits of the UDC. Since the UDC is designed as 11-bit,  $2^{11} - 1$  transistors are needed in this design. As shown in Figure 4.4, the gate terminals of the legs, which are driven by the UDC output bits, are interconnected in groups created by the exponents of two. In this way, each time the UDC counts up or down, only one leg is activated or deactivated in total. All legs are designed with minimum geometry and have a common drain and source connection. These *D* and *S* pins are also connected in parallel to the control transistors in the TRNG core. Custom-designed staged buffers that take place in this structure provide to drive the gates of legs faster. The size of these buffers should be increased from  $G_0$  to  $G_{10}$  due to the growing total capacitance seen from the total gate terminals of the legs.

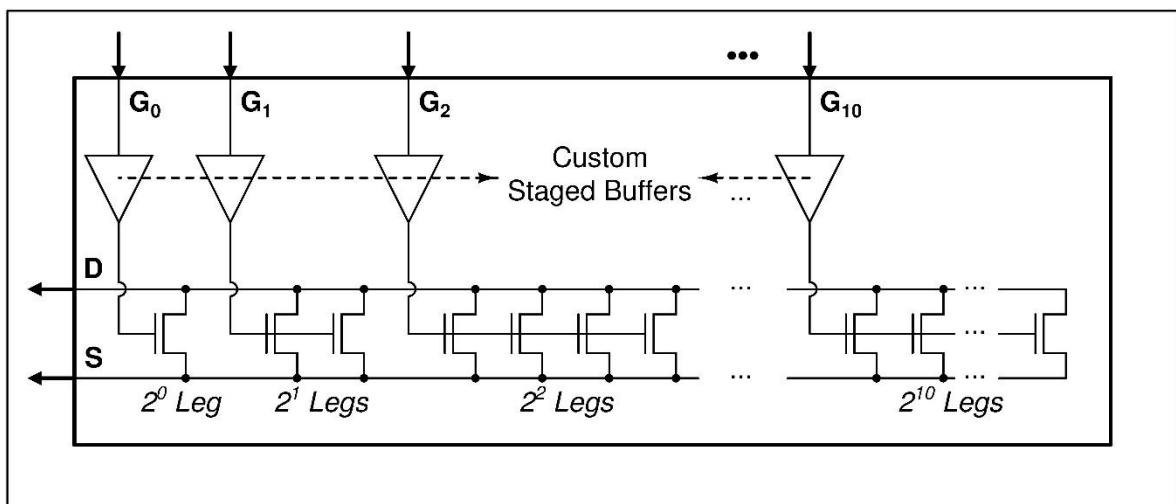


Figure 4.4. 11-Bit NMOS Parallel Legs

#### 4.6. CORRELATION SUPPRESSOR

A TRNG operating with a high Shannon Entropy does not mean that the quality of the random numbers is good. The presence of the serial correlation during bit generation reduces the quality of randomness. For this reason, post-processing is needed.

The Correlation Suppressor subcircuit consisting of an XOR gate, a 29-bit Serial In Serial Out (SISO) Shift Register, an 8-bit Serial In Parallel Out (SIPO) Shift Register, an 8-bit Parallel In Parallel Out (PIPO) Shift Register, and a Frequency Divider is demonstrated in Figure 4.5 [17,23]. One of the outputs of the TRNG is connected to the input pin of the Correlation Suppressor. In this way, this generated bit reaches the input of the XOR gate. The SISO Shift Register, whose input is connected to the XOR gate output, feeds its output to the second input of the XOR Gate with a feedback loop after restoring 29 bits. Thus, each bit produced in the TRNG is compared to the bit generated previous 29 clock cycles. After the XOR operation, the shifted bits are also transferred to the SIPO Shift Register. Meanwhile, The PIPO Shift Register receives the data from SIPO Shift Register. However, the PIPO Shift Register operates with a clock signal which is divided by 64 via the Frequency Divider. Therefore, 8-bit data contained in the 8-bit SIPO Shift Register are sampled at every 64 clock cycles by an 8-bit PIPO Shift Register. It is also convenient to use a Parallel In Serial Out (PISO) Shift Register instead of using a PIPO Shift Register to perform the same operation with a single bit output. However, in this process, an additional clock signal is needed to control the load and shift operations in SIPO Shift Register.

All the registers in the Correlation Suppressor have common preset and clear inputs. When TRNG is initially started to operate, it is recommended to reset the Correlation Suppressor by applying a ground pulse signal to its clear pin.

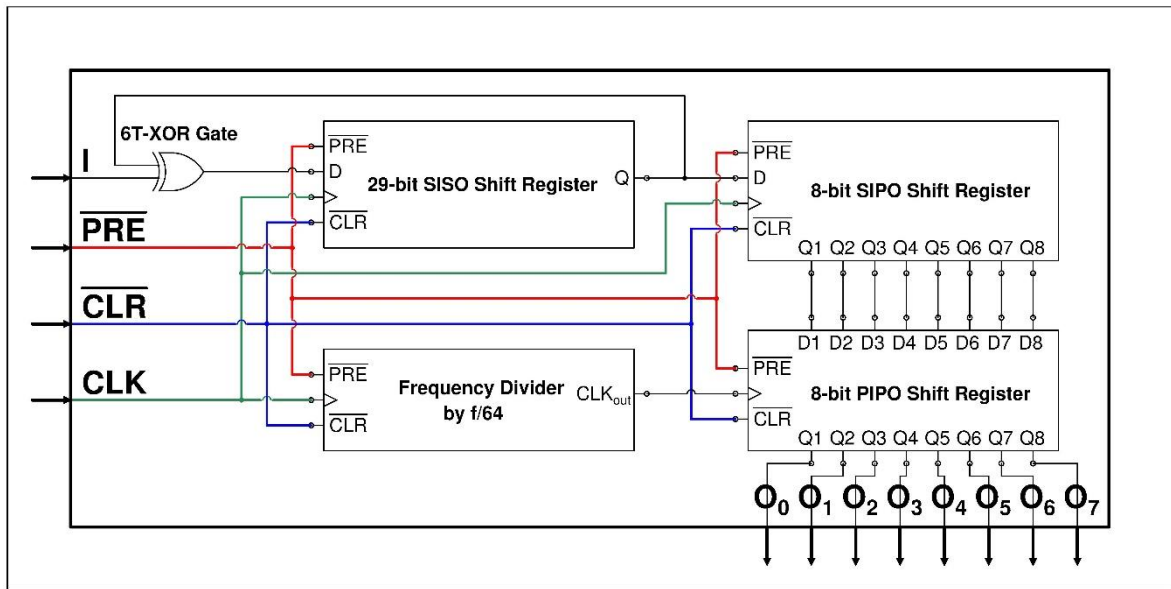


Figure 4.5. Correlation Suppressor with 8-bit output

#### 4.6.1. 6T-XOR Gate

The two-input XOR gate existing in the Correlation Suppressor consists of six transistors [24]. The electrical schematic of this custom logic gate is shown in Figure 4.6. The sizing values of the transistors are given in Table 4.7.

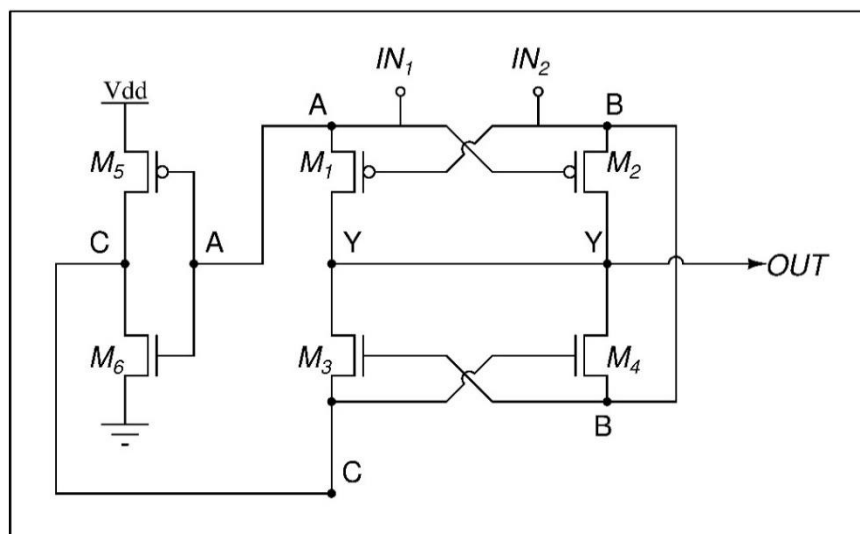


Figure 4.6. 2-input 6T-XOR gate

Table 4.7. Device sizes of 2-input 6T-XOR gate

| Device Name | Length | Width  |
|-------------|--------|--------|
| $M_1$       | 60 nm  | 460 nm |
| $M_2$       | 60 nm  | 115 nm |
| $M_3$       | 60 nm  | 320 nm |
| $M_4$       | 60 nm  | 80 nm  |
| $M_5$       | 60 nm  | 460 nm |
| $M_6$       | 60 nm  | 320 nm |

#### 4.6.2. SISO Shift Register

The SISO Shift Register consists of 29 serially connected registers. The input data is fed from the  $D$  pin of the first register. In each clock cycle, the output of the registers is shifted to the next register. Thus, the data at the pin  $D$  are transmitted to the pin  $Q$  after 29 clock periods. All the registers have a common preset and clear inputs. Besides, the clock inputs of the registers are common to behave a synchronous operation. The circuit schematic formed with the register subcircuits is indicated in Figure 4.7.

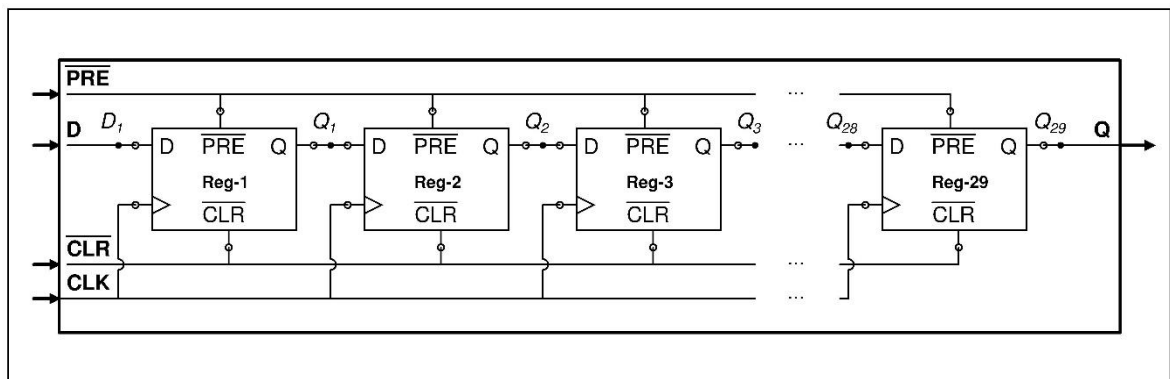


Figure 4.7. 29-Bit SISO Shift Register with preset and clear inputs

#### 4.6.3. SIPO Shift Register

Like the SISO Shift Register structure, the SIPO Shift Register consists of eight serially connected registers. Additionally, each register output is connected to the output pins to be used in a parallel manner. Its working principle is similar same with the SISO Shift Register. The circuit schematic formed with the register subcircuits is expressed in Figure 4.8.

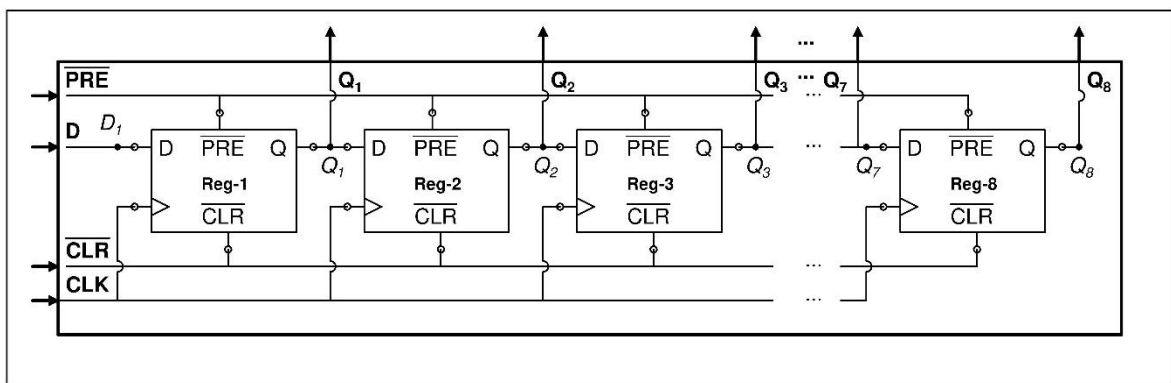


Figure 4.8. 8-Bit SIPO Shift Register with preset and clear inputs

#### 4.6.4. PIPO Shift Register

PIPO Shift Register consists of eight separate registers. *D* and *Q* pins of each register are used as input and output pins of PIPO. Since the clock signals are common, it performs a synchronous behavior. The circuit schematic formed with the register subcircuits is illustrated in Figure 4.9.

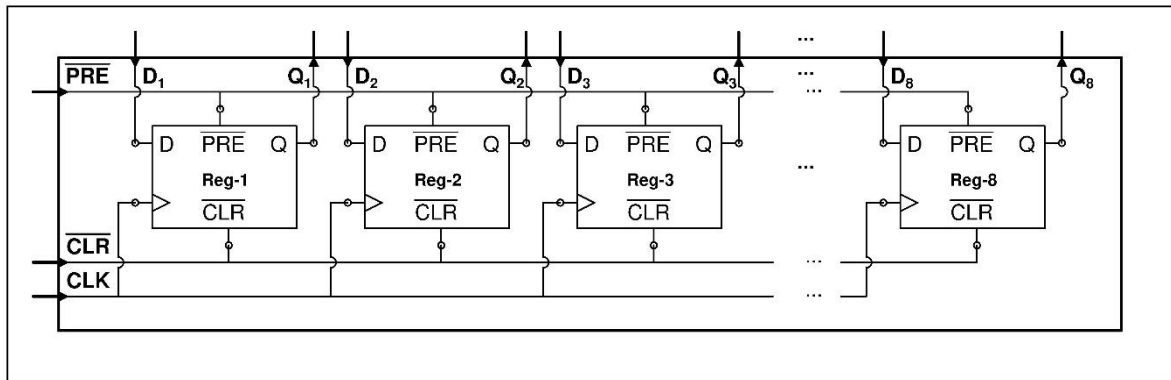


Figure 4.9. 8-Bit PIPO Shift Register with preset and clear inputs

#### 4.6.5. Frequency Divider

The Frequency Divider, which has an asynchronous structure, consists of six registers. The clock signal applied to this structure is connected to the clock pin of the first register. In each register,  $D$  and  $\bar{Q}$  pins are connected. This connection allows the register to generate a clock signal with half of the frequency of the applied clock signal at the output. Except for the first one, the registers receive their clock signal from the  $Q$  pin of the previous register. Therefore, a total of six registers are used for a clock division with  $f/64$  value. The circuit diagram with register subcircuit structures is shown in Figure 4.10.

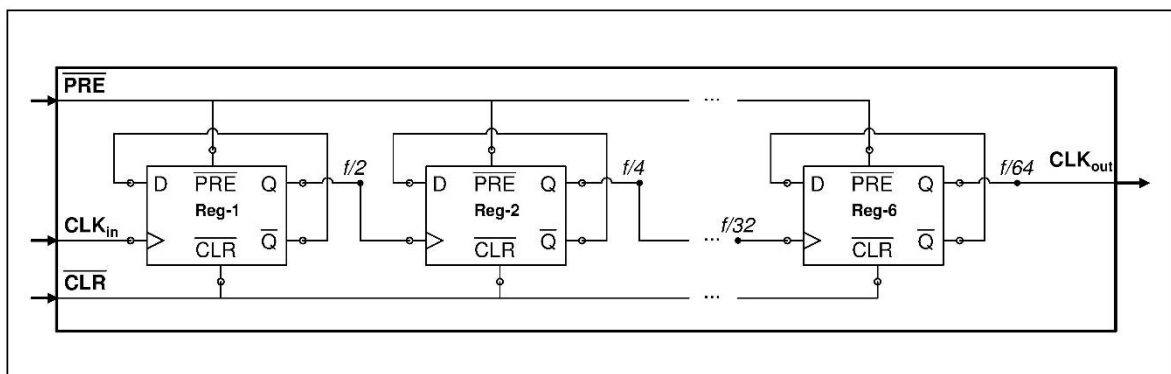


Figure 4.10. Frequency Divider by  $f/64$

## 4.7. CLOCK DELAYS

According to the design steps in Chapter 3, delayed clock signals are needed in the entire circuit. This operation is provided by Clock Delay Elements. Since two types of Clock Delay Circuits are needed, two different Clock Delay Elements are used and their usage number is adjusted according to the required delay time.

As a result of the design steps, using a master clock signal with a frequency of 100 MHz is suitable for the circuit to work properly.

### 4.7.1. Clock Delay Element

An even staged inverter chain can be used to create a delay element. When this structure is used, the same incoming signal is given to the output with a certain amount of propagation delay time. However, the delay time to be given to the clock signal in the design is much higher. Therefore, hundreds of inverters may be required to create the desired amount of delay using an inverter chain. Instead, with a customized structure, a much larger amount of delay can be obtained compared to a standard inverter. The circuit diagram of this structure called Clock Delay Element (CDE) is given in Figure 4.11. In this structure,  $M_{P2}$  and  $M_{N2}$ , whose gate terminals are at ground and supply voltage levels, are in conduction mode continuously. By connecting  $M_{P1}$  and  $M_{N1}$  in series to them, the first delayed stage of the CDE is formed. Therefore, the first stage acts as an inverter with a large delay consisting of four transistors. The amount of delay is provided by increasing the size of  $M_{P2}$  and  $M_{N2}$ .  $M_{P3}$  and  $M_{N3}$  transistors, which form the second stage of the CDE, are designed in small sizes and show a standard inverter behavior. The purpose of the second stage is to create a sharper square wave and also invert the inverted signal again. The pulse width of the clock signal to be generated using CDE is adjusted according to the  $T_{PHL}$  and  $T_{PLH}$  of the first stage. For this reason, to create signals with different pulse widths, the design is made by considering the  $J_{N(max)}/J_{P(max)}$  ratio, as in logic gates.

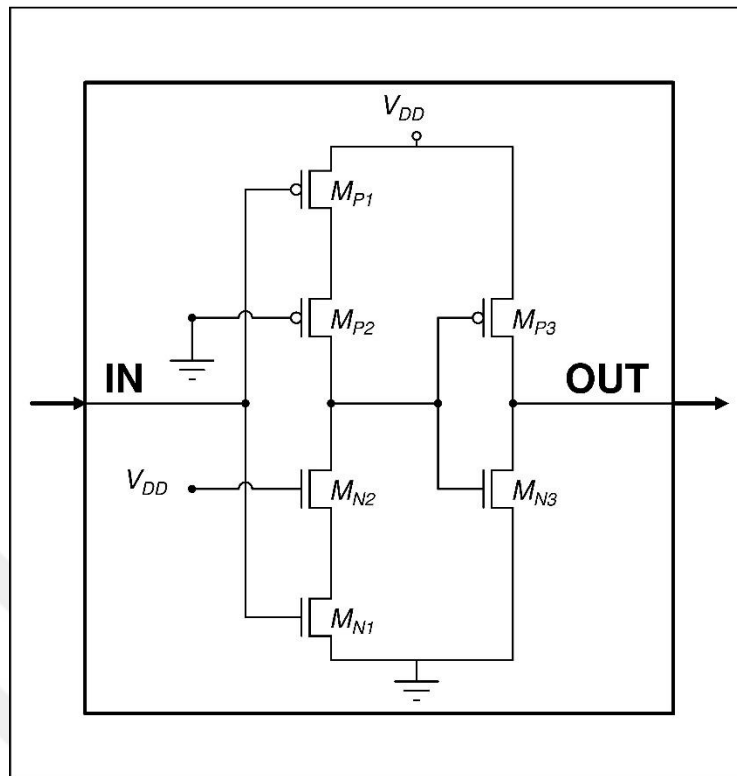


Figure 4.11. Clock Delay Element

One of the considerations in clock delay design is the amount of delay that needs to be adjusted. Instead of implementing the desired delay with a single CDE, using multiple CDEs having a smaller delay and connecting them in series provides a more PVT tolerant structure.

There are two different types of CDE structures in the entire circuit design. These are  $CDE_D$  to be used for registers and  $CDE_{FF}$  to be used for UDC. The pulse width of  $CDE_D$  is set to 50 percent, while the pulse width of  $CDE_{FF}$  is set to less than 50 percent. The dimensions of these two types of structures used are shown in Table 4.8.

Table 4.8. Device sizes of Clock Delay Element

| Type of CDE       | Device Name | Length | Finger Width | Finger Number | Total Width |
|-------------------|-------------|--------|--------------|---------------|-------------|
| CDE <sub>D</sub>  | $M_{P1}$    | 60 nm  | 165 nm       | 1             | 165 nm      |
|                   | $M_{N1}$    | 60 nm  | 80 nm        | 1             | 80 nm       |
|                   | $M_{P2}$    | 60 nm  | 165 nm       | 3             | 495 nm      |
|                   | $M_{N2}$    | 60 nm  | 80 nm        | 3             | 240 nm      |
|                   | $M_{P3}$    | 60 nm  | 165 nm       | 1             | 165 nm      |
|                   | $M_{N3}$    | 60 nm  | 80 nm        | 1             | 80 nm       |
| CDE <sub>FF</sub> | $M_{P1}$    | 60 nm  | 330 nm       | 1             | 330 nm      |
|                   | $M_{N1}$    | 60 nm  | 80 nm        | 1             | 80 nm       |
|                   | $M_{P2}$    | 60 nm  | 330 nm       | 3             | 990 nm      |
|                   | $M_{N2}$    | 60 nm  | 80 nm        | 1             | 80 nm       |
|                   | $M_{P3}$    | 60 nm  | 165 nm       | 1             | 165 nm      |
|                   | $M_{N3}$    | 60 nm  | 80 nm        | 1             | 80 nm       |

#### 4.7.2. Clock Delay Circuit

The Clock Delay Circuit (CDC) that creates the two different delayed clock signals needed in TRNG is shown in Figure 4.12. While eight CDE<sub>D</sub> blocks are used for the clock signal needed for the registers, 22 CDE<sub>FF</sub> blocks are used for the clock signal needed for UDCs. Two staged buffers are used so that the clock signals produced by the CDC can drive large capacitive loads on the nodes to which they are connected.

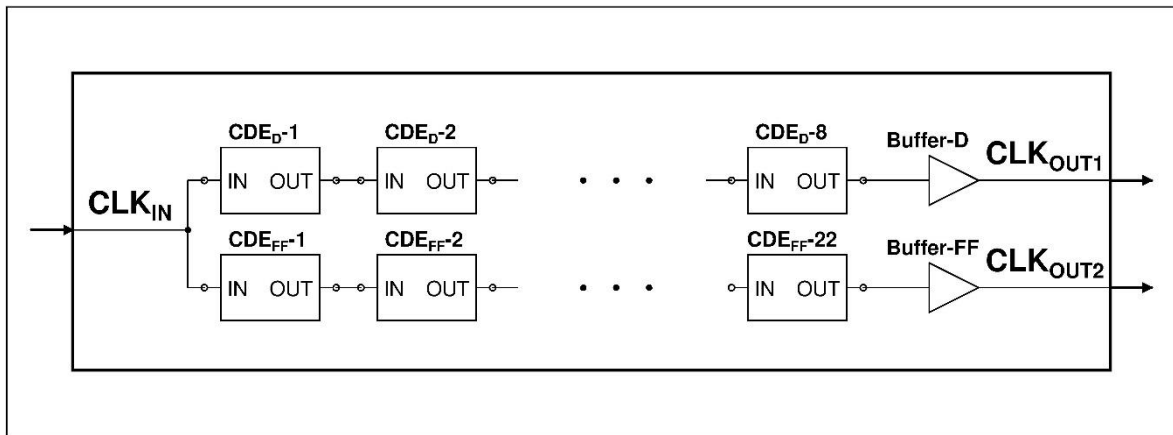


Figure 4.12. Clock Delay Circuit

#### 4.8. DESIGN CHARACTERISTICS

There is a tradeoff between the maximum offset compensation capability and the Shannon Entropy according to a specified size of SCL. Even if increasing the size of SCL provides more offset cancellation capability without changing the Shannon Entropy, it is not a good solution in terms of the size and the performance metrics of the TRNG.

$V_{DD}$  and  $V_{CM}$  pins of the TRNG are independent of each other. Although it is aimed to apply the maximum possible voltage to  $V_{CM}$  at the level of  $V_{DD}$ , there may be a need to slightly change the  $V_{CM}$  value in some circumstances. The common-mode voltage has a critical effect on the  $\sigma_n$  and  $V_{step}$  parameters. In cases with a high entropy value but insufficient offset compensation, the  $V_{step}$  value can be changed by reducing the  $V_{CM}$  and can be brought to a sufficient level for the offset compensation. When this process is being done, the  $\sigma_n$  decreases and the  $V_{step}$  increases. Therefore, it is very important to reduce the entropy value to a tolerable level. On the other hand, under the conditions where the entropy value is low and offset compensation can be done easily with a small number of steps, the  $V_{CM}$  value should be increased. In this case, the  $V_{CM}$  value must be increased to such an extent that compensation for the maximum expected offset value is guaranteed.

A remarkable solution that does not require the  $V_{CM}$  value to be manipulated is to connect the  $V_{CM}$  and  $V_{DD}$  pins. Thus, the voltage variation affects the  $V_{CM}$  and  $V_{DD}$  equally. From this point of view, the characteristics of the pre-layout design are examined in two different ways.

The first review deals with the situation where the  $V_{CM}$  value is constant at 1.2 V, while the second review deals with the situation where the  $V_{CM}$  is equal to the  $V_{DD}$  level. The metrics obtained as a result of the analyzes are explained in Section 4.8.1 and Section 4.8.2, respectively.

In this work, the characteristics of the TRNG were figured out on 45 different PVT corners. These corners consist of five different process corners, three different temperature corners, and three different supply voltage corners. Process corners consist of Fast NMOS - Fast PMOS (FF), Fast NMOS - Slow PMOS (FNSP), Slow NMOS - Fast PMOS (SNFP), Slow NMOS - Slow PMOS (SS), and Typical NMOS - Typical PMOS (TT). Voltage corners contain values of 1.1 V, 1.2 V, and 1.3 V, respectively. Temperature corners contain values of  $-40^{\circ}\text{C}$ ,  $27^{\circ}\text{C}$ , and  $125^{\circ}\text{C}$ , respectively.

#### 4.8.1. Fixed Common-Mode Voltage

In this section, noise RMS value, maximum offset cancellation capability, Shannon Entropy value, and offset voltage values were measured by keeping  $V_{CM}$  constant at 1.2 V.

The values of the RMS noise measurement on different PVT corners are shown in Table 4.9.

Table 4.9. RMS noise measurement with a fixed common-mode voltage

| $\sigma_n$ values at $V_{CM} = 1.2$ V |                       |                   |                   |                   |                   |                   |
|---------------------------------------|-----------------------|-------------------|-------------------|-------------------|-------------------|-------------------|
| Supply Voltage                        | Temperature           | Process           |                   |                   |                   |                   |
|                                       |                       | FF                | FNSP              | SNFP              | SS                | TT                |
| 1.1 V                                 | $-40^{\circ}\text{C}$ | 3.912 mV          | 3.993 mV          | 3.935 mV          | 3.985 mV          | 4.018 mV          |
|                                       | $27^{\circ}\text{C}$  | 4.045 mV          | 4.253 mV          | 3.967 mV          | 4.059 mV          | 4.135 mV          |
|                                       | $125^{\circ}\text{C}$ | 4.667 mV          | 4.657 mV          | 4.317 mV          | 4.189 mV          | 4.374 mV          |
| 1.2 V                                 | $-40^{\circ}\text{C}$ | 1.386 mV          | 1.317 mV          | 1.212 mV          | 1.187 mV          | 1.269 mV          |
|                                       | $27^{\circ}\text{C}$  | 1.535 mV          | 1.446 mV          | 1.284 mV          | 1.245 mV          | 1.353 mV          |
|                                       | $125^{\circ}\text{C}$ | 1.781 mV          | 1.659 mV          | 1.482 mV          | 1.428 mV          | 1.536 mV          |
| 1.3 V                                 | $-40^{\circ}\text{C}$ | 627 $\mu\text{V}$ | 592 $\mu\text{V}$ | 519 $\mu\text{V}$ | 497 $\mu\text{V}$ | 537 $\mu\text{V}$ |
|                                       | $27^{\circ}\text{C}$  | 743 $\mu\text{V}$ | 653 $\mu\text{V}$ | 577 $\mu\text{V}$ | 549 $\mu\text{V}$ | 601 $\mu\text{V}$ |
|                                       | $125^{\circ}\text{C}$ | 850 $\mu\text{V}$ | 760 $\mu\text{V}$ | 667 $\mu\text{V}$ | 626 $\mu\text{V}$ | 712 $\mu\text{V}$ |

While offset is being compensated in the design, a step is taken at the  $V_{step}$  value in each period. Therefore, the maximum amount of offset that the TRNG circuit can compensate, represented with  $V_{offc}$ , is achieved when the UDC on one side reaches the maximum number and all legs on that side are activated. Since 11-bit UDC is used, the  $V_{offc}$  value is 2047 times the  $V_{step}$  value. Table 4.10 gives the maximum offset values that TRNG can cancel out.

Table 4.10. Maximum offset cancellation capability with a fixed common-mode voltage

| <b><math>V_{offc}</math> values at <math>V_{CM} = 1.2</math> V</b> |                    |                |             |             |           |           |
|--------------------------------------------------------------------|--------------------|----------------|-------------|-------------|-----------|-----------|
| <b>Supply Voltage</b>                                              | <b>Temperature</b> | <b>Process</b> |             |             |           |           |
|                                                                    |                    | <b>FF</b>      | <b>FNSP</b> | <b>SNFP</b> | <b>SS</b> | <b>TT</b> |
| <b>1.1 V</b>                                                       | <b>−40 °C</b>      | 7 mV           | 6 mV        | 3 mV        | 1 mV      | 4 mV      |
|                                                                    | <b>27 °C</b>       | 11 mV          | 7 mV        | 3 mV        | 2 mV      | 5 mV      |
|                                                                    | <b>125 °C</b>      | 11 mV          | 8 mV        | 4 mV        | 3 mV      | 6 mV      |
| <b>1.2 V</b>                                                       | <b>−40 °C</b>      | 51 mV          | 47 mV       | 37 mV       | 31 mV     | 42 mV     |
|                                                                    | <b>27 °C</b>       | 54 mV          | 49 mV       | 39 mV       | 32 mV     | 43 mV     |
|                                                                    | <b>125 °C</b>      | 52 mV          | 48 mV       | 39 mV       | 33 mV     | 43 mV     |
| <b>1.3 V</b>                                                       | <b>−40 °C</b>      | 132 mV         | 143 mV      | 137 mV      | 145 mV    | 140 mV    |
|                                                                    | <b>27 °C</b>       | 137 mV         | 147 mV      | 142 mV      | 148 mV    | 145 mV    |
|                                                                    | <b>125 °C</b>      | 137 mV         | 146 mV      | 141 mV      | 146 mV    | 144 mV    |

Shannon Entropy values calculated based on the measured  $\sigma_n$  and  $V_{step}$  values are given in Table 4.11. In terms of entropy value, the worst corner appears at SS process, 1.3 V supply voltage, and −40 °C temperature. Even under this condition, a value higher than the target entropy value of 0.8 was obtained.

Table 4.11. Shannon Entropy calculation with a fixed common-mode voltage

| $H(x)$ values at $V_{CM} = 1.2$ V |             |         |        |        |        |        |
|-----------------------------------|-------------|---------|--------|--------|--------|--------|
| Supply Voltage                    | Temperature | Process |        |        |        |        |
|                                   |             | FF      | FNSP   | SNFP   | SS     | TT     |
| 1.1 V                             | −40 °C      | 0.999   | 0.9992 | 0.9996 | 0.9999 | 0.9994 |
|                                   | 27 °C       | 0.9985  | 0.9991 | 0.9996 | 0.9997 | 0.9993 |
|                                   | 125 °C      | 0.9987  | 0.999  | 0.9995 | 0.9996 | 0.9992 |
| 1.2 V                             | −40 °C      | 0.9795  | 0.9801 | 0.9829 | 0.9854 | 0.9815 |
|                                   | 27 °C       | 0.9804  | 0.9811 | 0.983  | 0.9856 | 0.9822 |
|                                   | 125 °C      | 0.9837  | 0.9838 | 0.9853 | 0.9871 | 0.9843 |
| 1.3 V                             | −40 °C      | 0.8864  | 0.8705 | 0.8591 | 0.8451 | 0.8607 |
|                                   | 27 °C       | 0.9     | 0.8789 | 0.8682 | 0.8562 | 0.8706 |
|                                   | 125 °C      | 0.9122  | 0.896  | 0.886  | 0.8747 | 0.8907 |

Finally, the measured offset voltage values are shown in Table 4.12. The  $V_{off}$  value, which is not much affected by the PVT variations, was observed as a maximum of 27 mV.

Table 4.12. Offset measurement with a fixed common-mode voltage

| $V_{off}$ values at $V_{CM} = 1.2$ V |             |         |         |         |         |       |
|--------------------------------------|-------------|---------|---------|---------|---------|-------|
| Supply Voltage                       | Temperature | Process |         |         |         |       |
|                                      |             | FF      | FNSP    | SNFP    | SS      | TT    |
| 1.1 V                                | −40 °C      | 25 mV   | 25 mV   | 27 mV   | 25 mV   | 25 mV |
|                                      | 27 °C       | 25 mV   | 25 mV   | 25.5 mV | 25.5 mV | 24 mV |
|                                      | 125 °C      | 23 mV   | 24 mV   | 24.5 mV | 24 mV   | 24 mV |
| 1.2 V                                | −40 °C      | 24 mV   | 24.5 mV | 25 mV   | 24 mV   | 24 mV |
|                                      | 27 °C       | 24 mV   | 23.5 mV | 24 mV   | 24.5 mV | 25 mV |
|                                      | 125 °C      | 23.5 mV | 24 mV   | 23 mV   | 24 mV   | 24 mV |
| 1.3 V                                | −40 °C      | 25 mV   | 24.5 mV | 23 mV   | 25 mV   | 25 mV |
|                                      | 27 °C       | 24 mV   | 24 mV   | 23.5 mV | 25 mV   | 24 mV |
|                                      | 125 °C      | 23 mV   | 24 mV   | 23.5 mV | 24.5 mV | 24 mV |

When Table 4.10 and Table 4.12 are compared, it is clear that the offset compensation is insufficient in a total of 15 corners where TRNG operates with a 1.1 V supply voltage level.

#### 4.8.2. Varying Common-Mode Voltage

The characteristics mentioned in the previous section are reviewed again in this section where  $V_{CM}$  is equal to  $V_{DD}$ . The corners where the supply voltage value is 1.2 V are ignored because they are common in both sections.

The values of the RMS noise measurement are given in Table 4.13.

Table 4.13. RMS noise measurement with a varying common-mode voltage

| $\sigma_n$ values at $V_{CM} = V_{DD}$ |             |          |          |          |          |          |
|----------------------------------------|-------------|----------|----------|----------|----------|----------|
| Supply Voltage                         | Temperature | Process  |          |          |          |          |
|                                        |             | FF       | FNSP     | SNFP     | SS       | TT       |
| 1.1 V                                  | −40 °C      | 1.419 mV | 1.372 mV | 1.239 mV | 1.225 mV | 1.295 mV |
|                                        | 27 °C       | 1.57 mV  | 1.46 mV  | 1.325 mV | 1.282 mV | 1.368 mV |
|                                        | 125 °C      | 1.828 mV | 1.7 mV   | 1.493 mV | 1.479 mV | 1.609 mV |
| 1.3 V                                  | −40 °C      | 1.386 mV | 1.298 mV | 1.19 mV  | 1.17 mV  | 1.255 mV |
|                                        | 27 °C       | 1.519 mV | 1.439 mV | 1.261 mV | 1.23 mV  | 1.325 mV |
|                                        | 125 °C      | 1.758 mV | 1.643 mV | 1.46 mV  | 1.385 mV | 1.513 mV |

Table 4.14 shows the maximum offset values that the TRNG can compensate.

Table 4.14. Maximum offset cancellation capability with a varying common-mode voltage

| $V_{offc}$ values at $V_{CM} = V_{DD}$ |             |         |       |       |       |       |
|----------------------------------------|-------------|---------|-------|-------|-------|-------|
| Supply Voltage                         | Temperature | Process |       |       |       |       |
|                                        |             | FF      | FNSP  | SNFP  | SS    | TT    |
| 1.1 V                                  | −40 °C      | 50 mV   | 46 mV | 36 mV | 29 mV | 40 mV |
|                                        | 27 °C       | 52 mV   | 47 mV | 37 mV | 30 mV | 41 mV |
|                                        | 125 °C      | 50 mV   | 46 mV | 37 mV | 31 mV | 41 mV |
| 1.3 V                                  | −40 °C      | 52 mV   | 49 mV | 38 mV | 32 mV | 43 mV |
|                                        | 27 °C       | 55 mV   | 51 mV | 40 mV | 34 mV | 45 mV |
|                                        | 125 °C      | 53 mV   | 51 mV | 40 mV | 35 mV | 44 mV |

Shannon Entropy values calculated as a result of the values measured in Table 4.13 and Table 4.14 are given in Table 4.15.

Table 4.15. Shannon Entropy calculation with a varying common-mode voltage

| $H(x)$ values at $V_{CM} = V_{DD}$ |             |         |        |        |        |        |
|------------------------------------|-------------|---------|--------|--------|--------|--------|
| Supply Voltage                     | Temperature | Process |        |        |        |        |
|                                    |             | FF      | FNSP   | SNFP   | SS     | TT     |
| 1.1 V                              | −40 °C      | 0.9803  | 0.9813 | 0.9838 | 0.9867 | 0.9827 |
|                                    | 27 °C       | 0.9815  | 0.982  | 0.9844 | 0.9869 | 0.9832 |
|                                    | 125 °C      | 0.9847  | 0.9849 | 0.9861 | 0.9883 | 0.9857 |
| 1.3 V                              | −40 °C      | 0.9791  | 0.9789 | 0.9822 | 0.9847 | 0.9809 |
|                                    | 27 °C       | 0.9798  | 0.9802 | 0.9823 | 0.9845 | 0.981  |
|                                    | 125 °C      | 0.9831  | 0.9827 | 0.9847 | 0.9859 | 0.9837 |

As can be seen from Table 4.15, the entropy values obtained at all PVT corners by equating the common-mode voltage to the supply voltage are close to each other and around 0.98.

Finally, the measured offset voltage values are shown in Table 4.16.

Table 4.16. Offset voltage measurement with a varying common-mode voltage

| $V_{off}$ values at $V_{CM} = V_{DD}$ |             |         |         |         |         |         |
|---------------------------------------|-------------|---------|---------|---------|---------|---------|
| Supply Voltage                        | Temperature | Process |         |         |         |         |
|                                       |             | FF      | FNSP    | SNFP    | SS      | TT      |
| 1.1 V                                 | −40 °C      | 25.5 mV | 25 mV   | 25.5 mV | 26 mV   | 26.5 mV |
|                                       | 27 °C       | 23.5 mV | 25 mV   | 25 mV   | 25.5 mV | 25 mV   |
|                                       | 125 °C      | 23 mV   | 25.5 mV | 24.5 mV | 25.5 mV | 24 mV   |
| 1.3 V                                 | −40 °C      | 25 mV   | 25 mV   | 23 mV   | 23 mV   | 22.5 mV |
|                                       | 27 °C       | 23.5 mV | 24.5 mV | 24 mV   | 24.5 mV | 23 mV   |
|                                       | 125 °C      | 23 mV   | 23.5 mV | 23 mV   | 23.5 mV | 23 mV   |

Comparing Table 4.14 and Table 4.16, it appears that TRNG can provide the offset compensation at all corners. However, the worst corner for the  $V_{offc}$ , which includes SS process, −40 °C temperature, and 1.1 V supply voltage, has a critical value. When parasitics are extracted after layout, the offset compensation may not be fully eliminated with a 100 percent probability. In such a case, lowering the  $V_{CM}$  to a small extent solves this problem.

As a result, equalizing the  $V_{CM}$  to the  $V_{DD}$  level provides the offset cancellation with a very high probability at all corners, as well as a high entropy value.

#### 4.9. TRNG CIRCUIT LAYOUT

Since TRNGs usually form a part of a different circuit, the drawn layout does not include a top-level layout. Therefore, output buffers should be added to the 8-bit outputs of the TRNG, taking into account the input capacitances of the circuit that will use this structure. If a single TRNG chip is to be taped out, the pad frames should be designed and input and output buffers should be created accordingly.

The layout of the designed TRNG circuit is shown in Figure 4.13. Except for the Correlation Suppressor subcircuit, the entire circuit has a symmetrical structure. Thus, the layout of the TRNG circuit was also designed symmetrically. Especially, the TRNG Core part was assumed as an analog circuit and the layout was made by following the physical design rules. The entire layout was drawn using five metal layers.

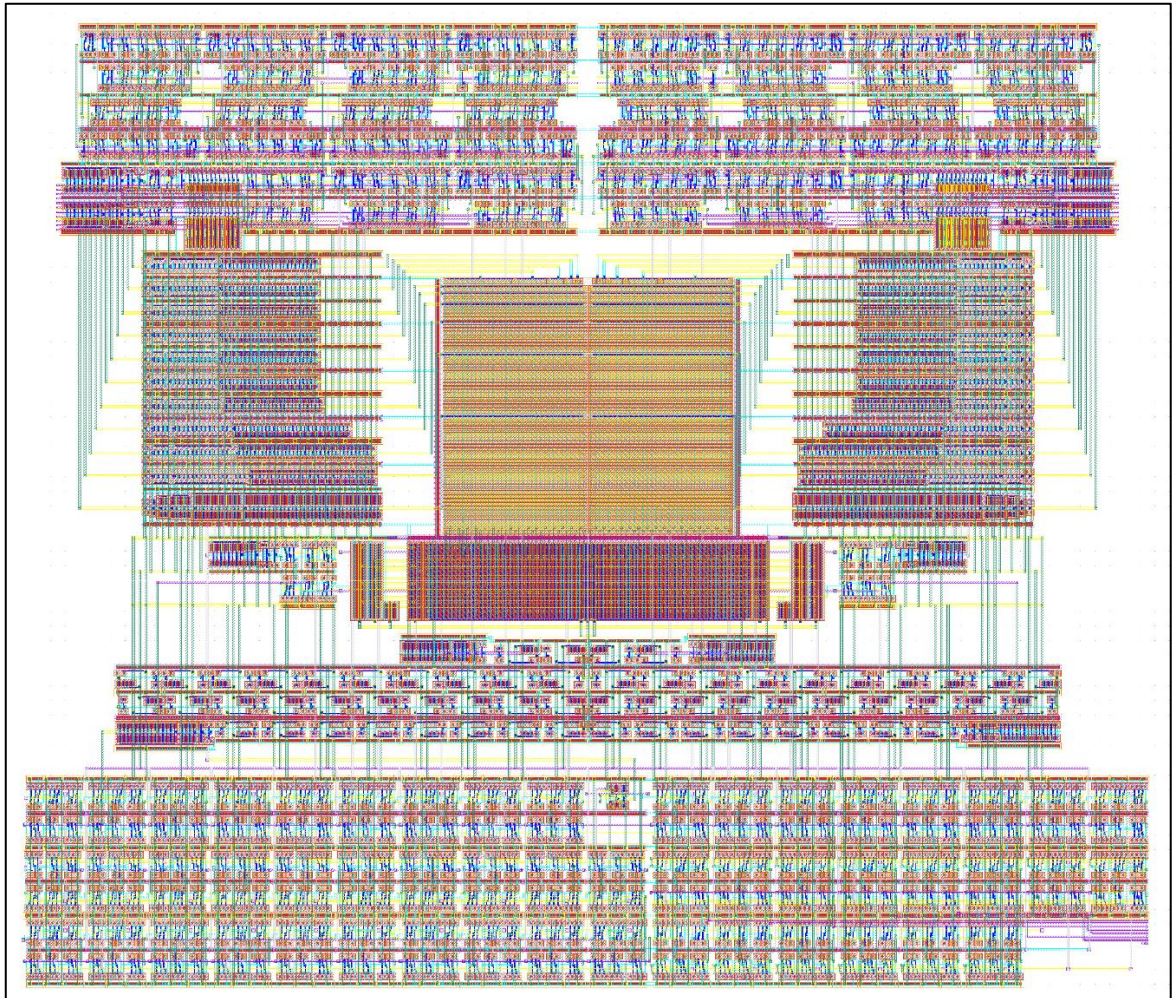


Figure 4.13. Layout of the TRNG

Some parts of the TRNG layout are also indicated in Figure 4.14. The die size appears to be  $4881 (\mu\text{m})^2$ .

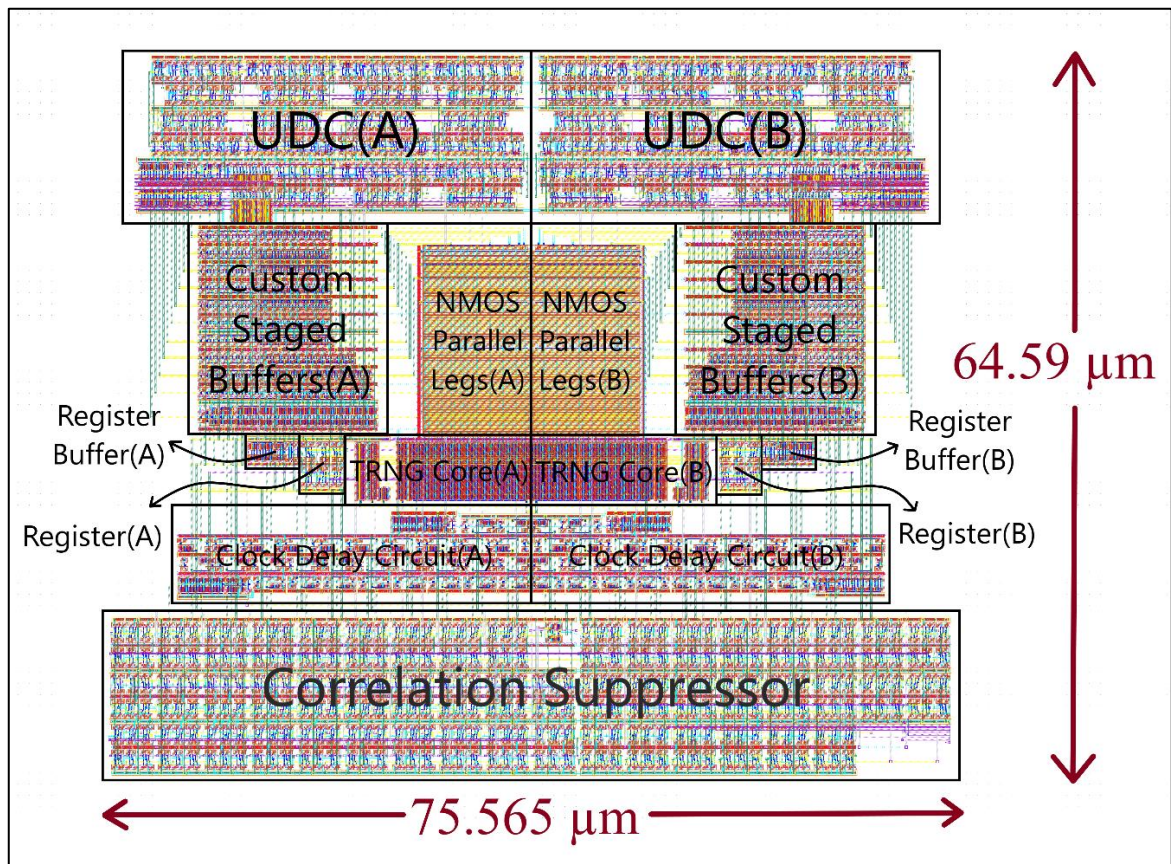


Figure 4.14. Layout of the TRNG represented with the circuit blocks

## 5. VERIFICATION

### 5.1. POST-LAYOUT SIMULATION

After the layout of the TRNG is drawn, the parasitics are extracted. Post-layout simulations which include the parasitic effects should be run to verify whether the circuit works as desired. It is examined in Section 5.1.1 whether the applied clock signal and the designed clock delays are sufficient for the TRNG to work properly. On the other hand, whether the maximum offset that may occur in the TRNG can be eliminated is inspected in Section 5.1.2.

#### 5.1.1. Timing Diagram

The timing diagram was reviewed on three different corners. Except for the nominal case, the corners where the delays are the most and the least are the PVT corners involving SS, 1.1 V, 125 °C and FF, 1.3 V, -40 °C, respectively.

During the examinations, the transient analysis was performed for a total of four clock periods. Initially, a clear signal was applied to both UDCs. Also, in the reset phase of the third period, a preset signal was applied to the UDC-A. In this way, it was also observed whether the propagation delays of all UDC outputs are close to each other.

In Figure 5.1, the timing diagram of the best corner is given. “UDC\_A” and “UDC\_B” values at the top of the figure represent the count value of the UDCs in decimal number base. The “CLK”, “PRE”, and “CLR” signals represent the main clock signal applied to the TRNG, the preset signal applied to the UDC-A, and the clear signal applied to both UDCs, respectively. “VOA” and “VOB” values indicate the TRNG core outputs, where “QA” and “QB” values point out the register outputs related to the TRNG core outputs. The signals “PHI2\_A”, “PHI2\_B”, “PHI3\_A”, and “PHI3\_A” illustrate the delayed clock signals generated by the Clock Delay Circuits in parts A and B of TRNG. Finally, the signals starting with “p\_Q” at the bottom express the output signals of the UDC-A. Since the names of 11 UDC outputs do not fit in the graph, the names of the first three bits are shown.

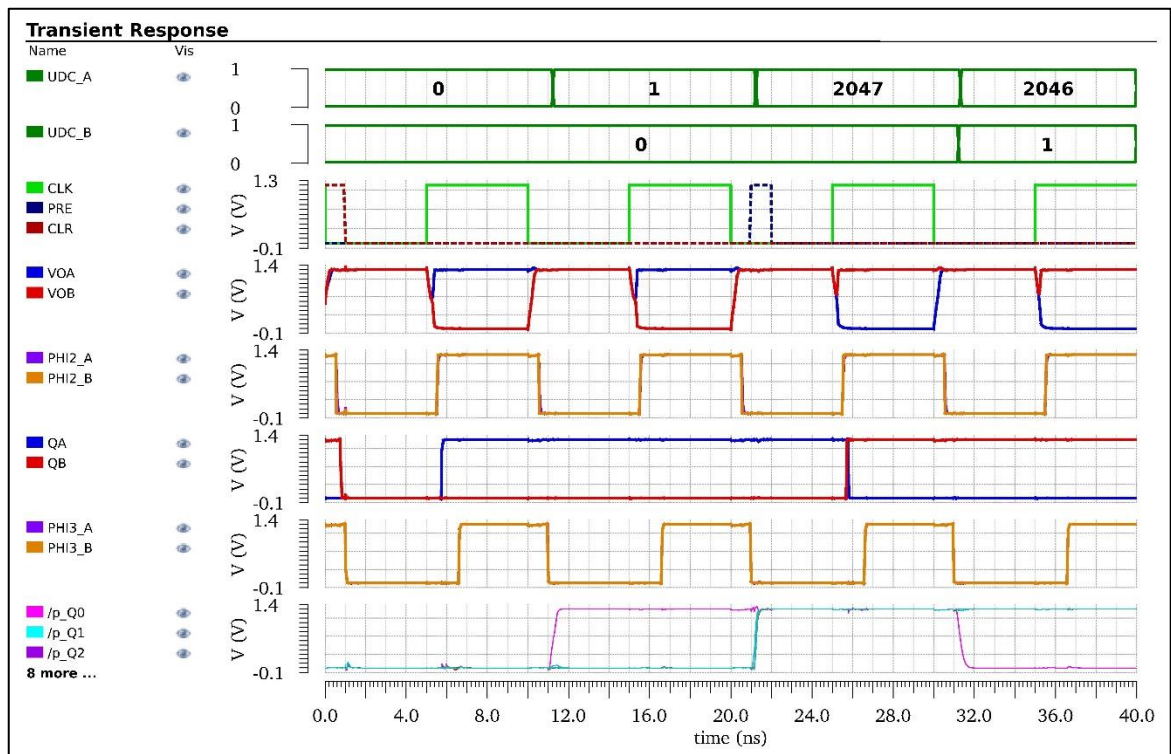


Figure 5.1. Timing diagram of the TRNG on the best corner

The timing diagram of the nominal corner is shown in Figure 5.2. The signals in the graph are the same as in Figure 5.1

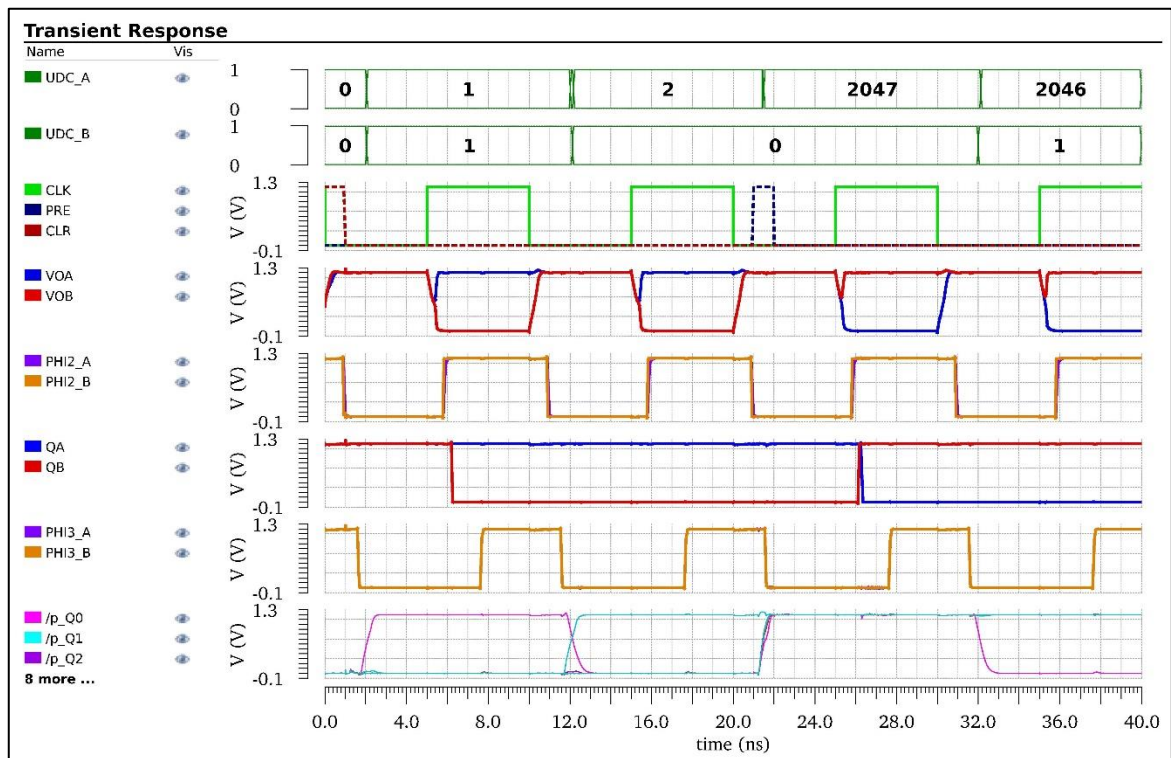


Figure 5.2. Timing diagram of the TRNG on the nominal corner

The timing diagram of the worst corner is shown in Figure 5.3. The signals in the graph are the same as in Figure 5.1 and Figure 5.2.

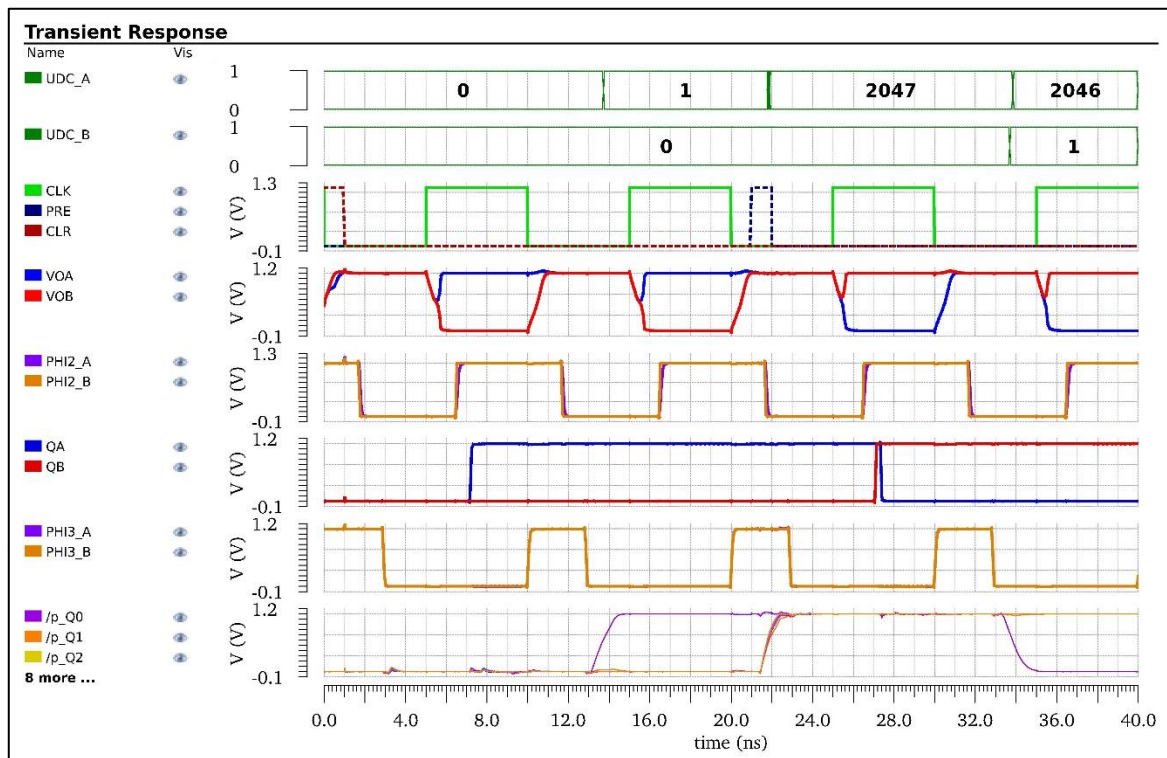


Figure 5.3. Timing diagram of the TRNG on the worst corner

### 5.1.2. Offset Compensation Test

Since it is not possible to place any circuit element inside the entire circuit for testing purposes after layout, it can be observed with a performing Monte Carlo analysis whether the offset can be removed or not. While the offset is being compensated, the UDC on the one side waits at zero value, while the other one counts in the forward direction. Since a different offset value will occur at each point in the Monte Carlo sampling, it is expected that the counting UDC will reach a different count value at any point. As it is not known how much offset will occur at which point, it is necessary to run a transient analysis long enough for the UDC to reach its maximum value. As a transient simulation including at least 2047 clock periods would take a long time for a TRNG with 11-bit UDC, applying a preset signal to the UDC on one side shortens the simulation time. Assuming a preset signal is applied to the UDC-A, maximum offset cancellation capability is provided in the A part of the TRNG. If the  $V_{offc}$  is above the resulting offset value, bit-0 is expected at the OA output of the TRNG and bit-1 is expected at the OB output.

Offset compensation tests were performed on three different PVT corners. These corners consist of FF, 1.3 V, 125 °C for the best corner, TT, 1.2 V, 27 °C for the nominal corner, and SS, 1.1 V, -40 °C for the worst corner in terms of  $V_{offc}$  value examined in Chapter 5. Simulations were performed in the  $V_{DD} = V_{CM}$  condition, which shows a more stable performance on the PVT corners.

All Monte Carlo analyzes were performed at  $3\sigma$  corners and 1000 sampling points. A transient simulation including a two-clock period stop time was set for the Monte Carlo analysis. All the  $V_{OA}$  and  $V_{OB}$  values, which are the output voltages of the TRNG core, were plotted as a family plot after the simulations. Test setup includes a preset signal applied to the UDC-A before the second clock period. Therefore, the outputs of the TRNG core reach  $V_{DD}$  or ground within the range of 15 ns - 20 ns, which is the time interval of the second evaluation phase.

The offset compensation test result for the best corner is shown in Figure 5.4. By reason of the signal names of 1000 Monte Carlo points do not fit in the graph, the signals of the first 16 points for both TRNG core outputs are shown in the graph. As can be seen from the graph,  $V_{OA}$  values reach bit-0 while the  $V_{OB}$  values are at bit-0 for all Monte Carlo points. Therefore, the offset cancellation is completely successful.

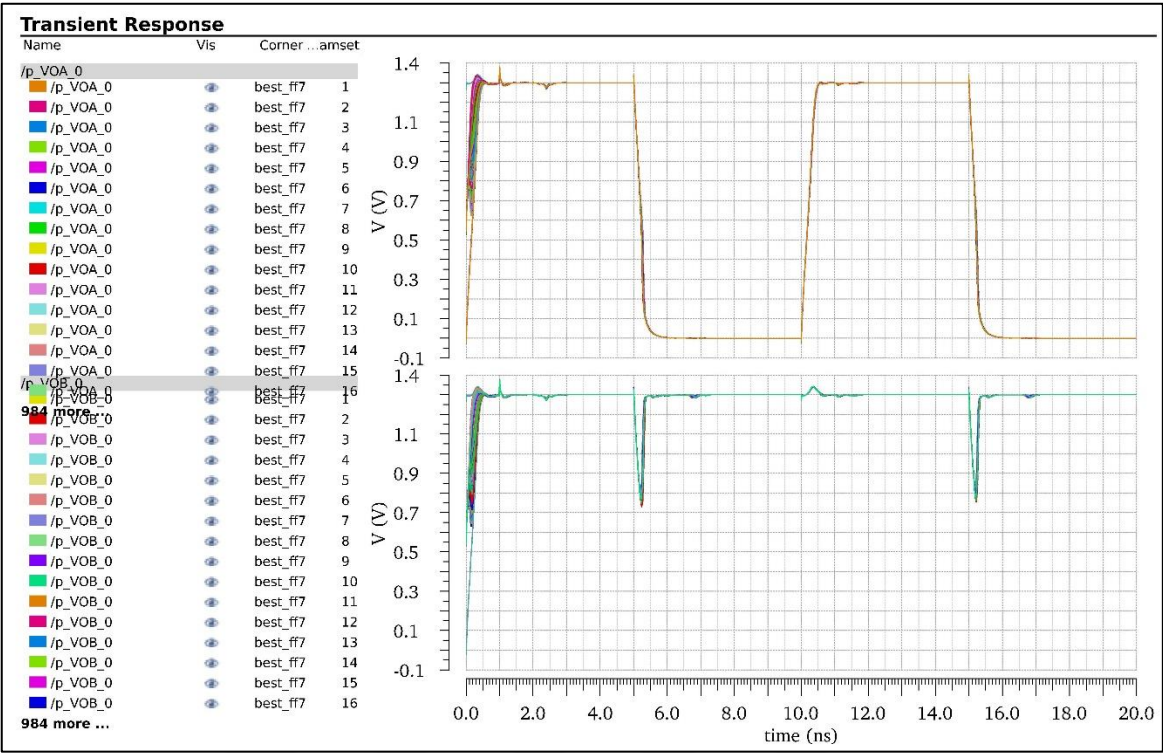


Figure 5.4. Offset compensation test for the best corner

Similarly, the simulation result for the nominal corner is given in Figure 5.5. Here, the offset compensation also appears to be completely successful.

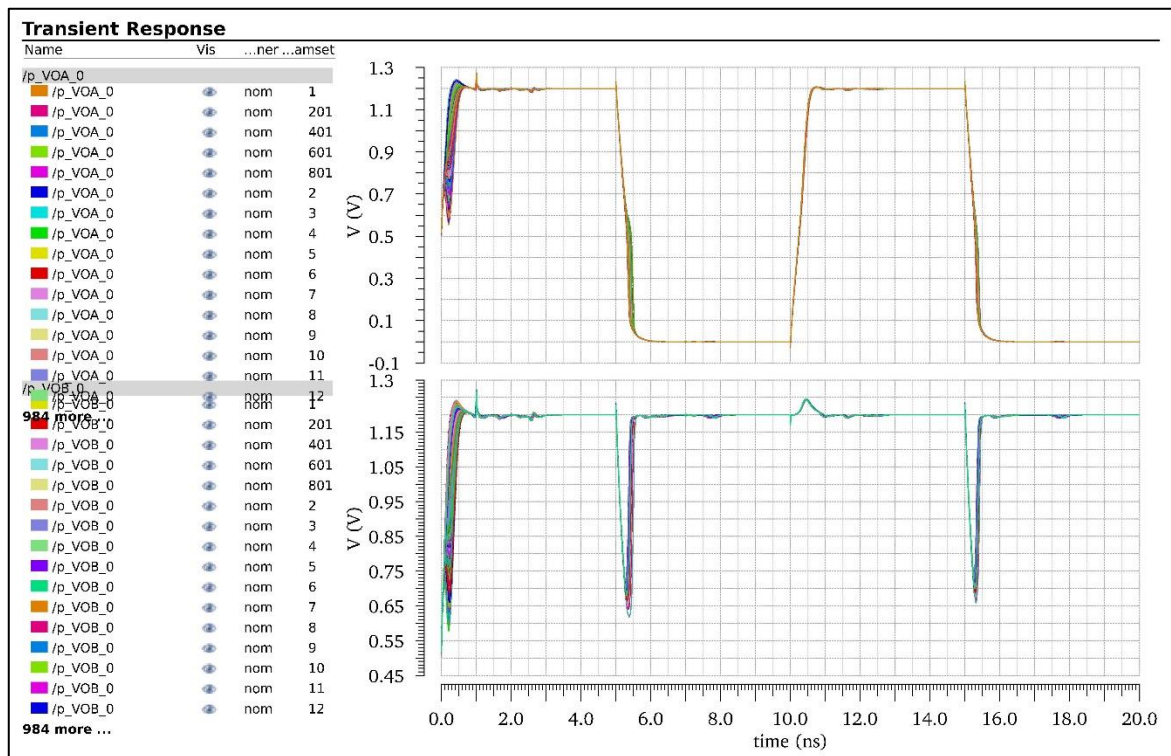


Figure 5.5. Offset compensation test for the nominal corner

The simulation result for the worst case is indicated in Figure 5.6. In this graph, 15 of  $V_{OA}$  values over 1000 Monte Carlo points reach bit-1. In this most critical corner, offset compensation is provided with a 98.5 percent probability. Therefore, a smaller  $V_{CM}$  independent of  $V_{DD}$  needs to be applied to ensure that the TRNG works properly even in the worst case.

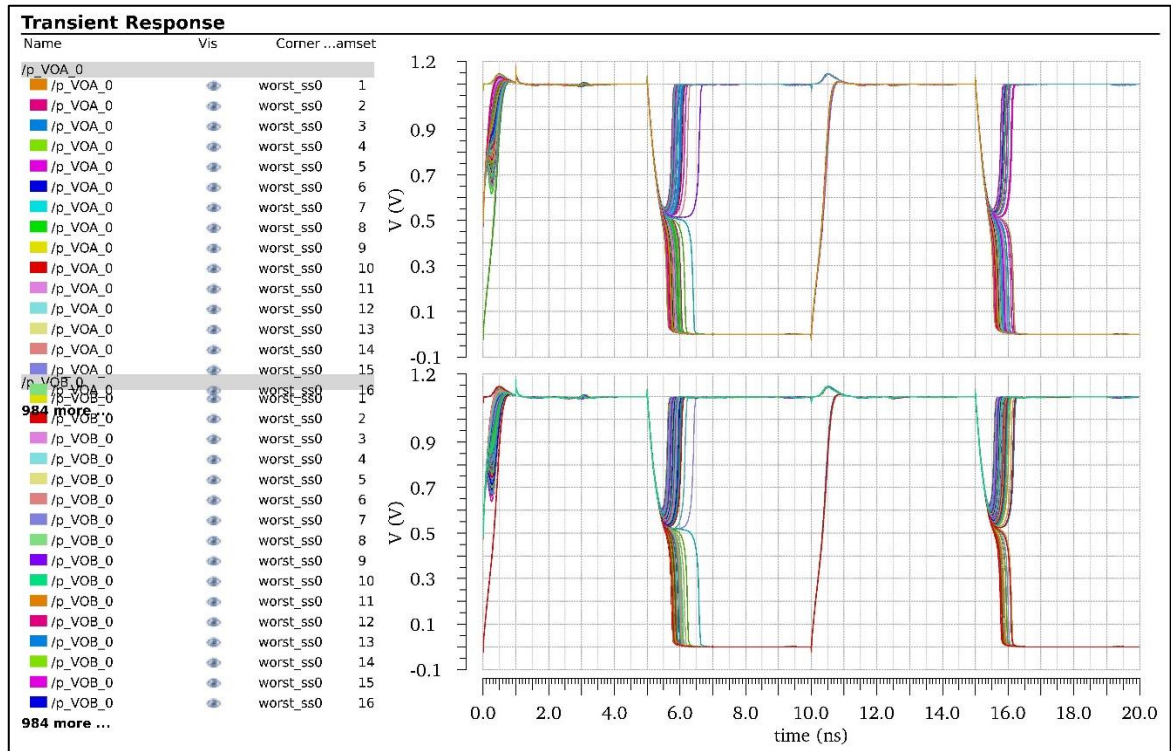


Figure 5.6. Offset compensation test for the worst corner

The common-mode voltage has been reduced from 1.1 V to 1.05 V in order to fully satisfy the offset compensation at the worst corner. The results obtained after this adjustment are demonstrated in Figure 5.7. It is clear that a 50 mV drop in  $V_{CM}$  fully provides the offset compensation.

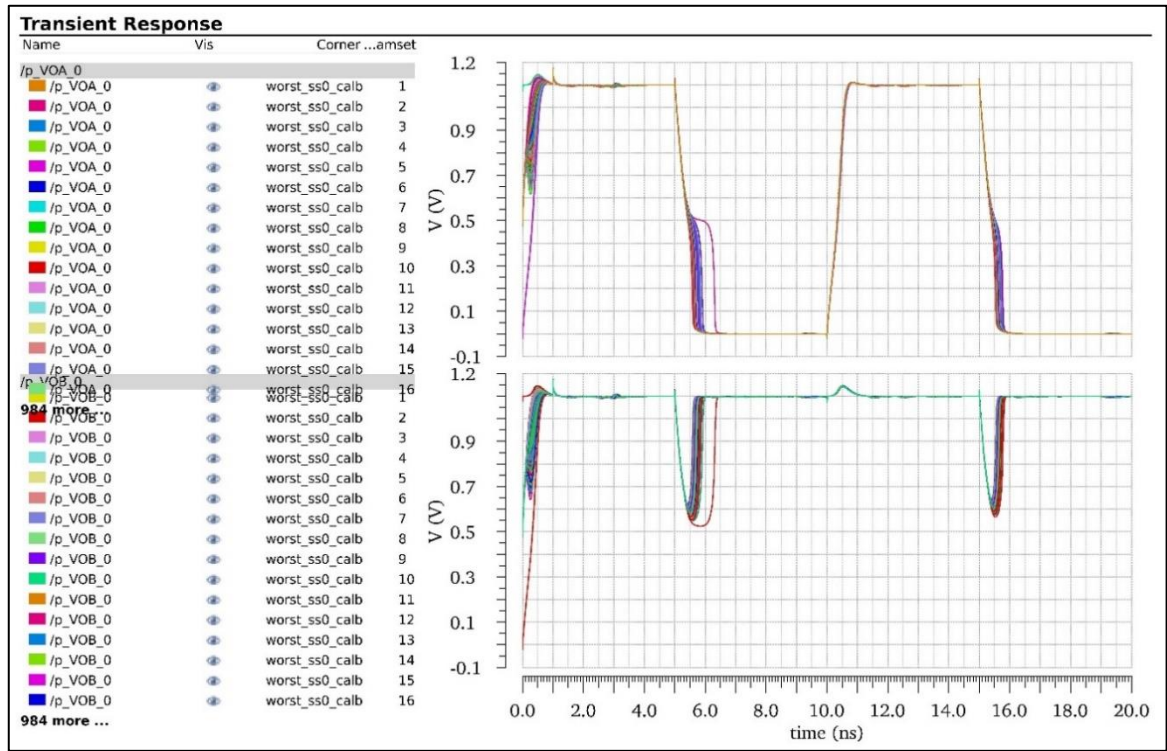


Figure 5.7. Calibrated offset compensation test for the worst corner

## 5.2. RANDOMNESS TEST

For a TRNG to be used in cryptographic applications, some statistical randomness tests must be applied to the numbers generated in the TRNG. The statistical test suite prepared by NIST is very suitable for this operation [25]. For randomness tests, usually, a bitstream containing 1 million bits is tested. This bitstream is recorded by measuring the outputs of the designed TRNG chip after it is manufactured and then put into the randomness tests in the computer environment.

In this study, the tapeout of the proposed design was not fabricated. For this reason, the bitstream required for the randomness test was obtained with a long transient simulation. Enabling the noise option in transient analysis extremely extends the simulation time. In addition, since the throughput of the TRNG is reduced by eight times due to the post-processor, a transient simulation should be run over at least 8 million clock periods. Moreover, if a post-layout simulation including parasitics is desired, the simulation time

may take thousands of years on an average-speed computer. Therefore, the reductions made to obtain such a large bitstream with simulation are as follows:

- A pre-layout simulation was run instead of a post-layout simulation.
- Although the Correlation Suppressor circuit is implemented as hardware to the TRNG, the same post-processing operation can be performed through software. Hence, the Correlation Suppressor structure was removed from the entire circuit.
- Spectre® XPS MS was used as a high-performance simulator. In the simulation settings, TRNG core, NMOS Parallel Legs, and registers sampling TRNG core were marked as an analog subcircuit, while all remaining circuit blocks were marked as a digital subcircuit. Maximum digital speed was used.
- A transient analysis having at least an 8 million clock period stop time was formed. After enabling the transient noise option, 50 GHz was assigned as the “Noise Fmax” value. In the “Accuracy Defaults” section, “moderate” was selected.

After the simulation was completed, one of the register outputs which is connected to the TRNG core output was plotted. This signal was digitally sampled at each clock cycle to extract the bitstream including 8 million bits. Then the bitstream was post-processed through MATLAB® software. The corresponding MATLAB code is available in Appendix A. Finally, the obtained 1 million bit length bitstream was tested under the NIST test suite.

Before the post-processing, 4000122 zeros and 3999878 ones were counted in 8 million raw bitstream. Based on these values, the Shannon Entropy value for the raw bitstream was calculated as 0.999999999328967. When it was put into the NIST test, it passed only 5 out of 15 randomness tests. For this reason, post-processing is essential for this design.

After post-processing operation, 499802 zeros and 500198 ones were observed. The corresponding Shannon Entropy value was calculated as 0.99999886881164. NIST test results of the post-processed data are given in Table 5.1. As seen in the table, TRNG passed all NIST tests successfully after post-processing.

Table 5.1. NIST test results

| NIST Test                    | P-value  | Result               | Details                                                                                                   |
|------------------------------|----------|----------------------|-----------------------------------------------------------------------------------------------------------|
| Approximate Entropy          | 0.231671 | SUCCESS              | -                                                                                                         |
| Block Frequency              | 0.371160 | SUCCESS              | -                                                                                                         |
| Cumulative Sums              | 0.959109 | SUCCESS<br>(2/2)     | P-value(Forward) = 0.879009<br>P-value(Reverse) = 0.959109                                                |
| FFT                          | 0.520637 | SUCCESS              | -                                                                                                         |
| Frequency                    | 0.692105 | SUCCESS              | -                                                                                                         |
| Linear Complexity            | 0.886171 | SUCCESS              | -                                                                                                         |
| Longest Run                  | 0.597547 | SUCCESS              | -                                                                                                         |
| Non-Overlapping<br>Template  | 0.992825 | SUCCESS<br>(148/148) | 148 Different Templates<br>110100100, P-value(min) =<br>0.016133<br>111000100, P-value(max) =<br>0.992825 |
| OverlappingTemplate          | 0.967914 | SUCCESS              | -                                                                                                         |
| Random Excursions            | 0.879506 | SUCCESS<br>(8/8)     | from $x = -4$ to $x = 4$<br>$x = 3$ , P-value(min) = 0.114545<br>$x = 1$ , P-value(max) = 0.879506        |
| Random Excursions<br>Variant | 0.990581 | SUCCESS<br>(18/18)   | from $x = -9$ to $x = 9$<br>$x = -4$ , P-value(min) = 0.080904<br>$x = 7$ , P-value(max) = 0.990581       |
| Rank                         | 0.925766 | SUCCESS              | -                                                                                                         |
| Runs                         | 0.070631 | SUCCESS              | -                                                                                                         |
| Serial                       | 0.069772 | SUCCESS<br>(2/2)     | P-value(1) = 0.064249<br>P-value(2) = 0.069772                                                            |
| Universal                    | 0.279694 | SUCCESS              | -                                                                                                         |

The image of the bitstream obtained after post-processing is displayed in Figure 5.8. In this image, black dots represent bit-0, while white dots represent bit-1.

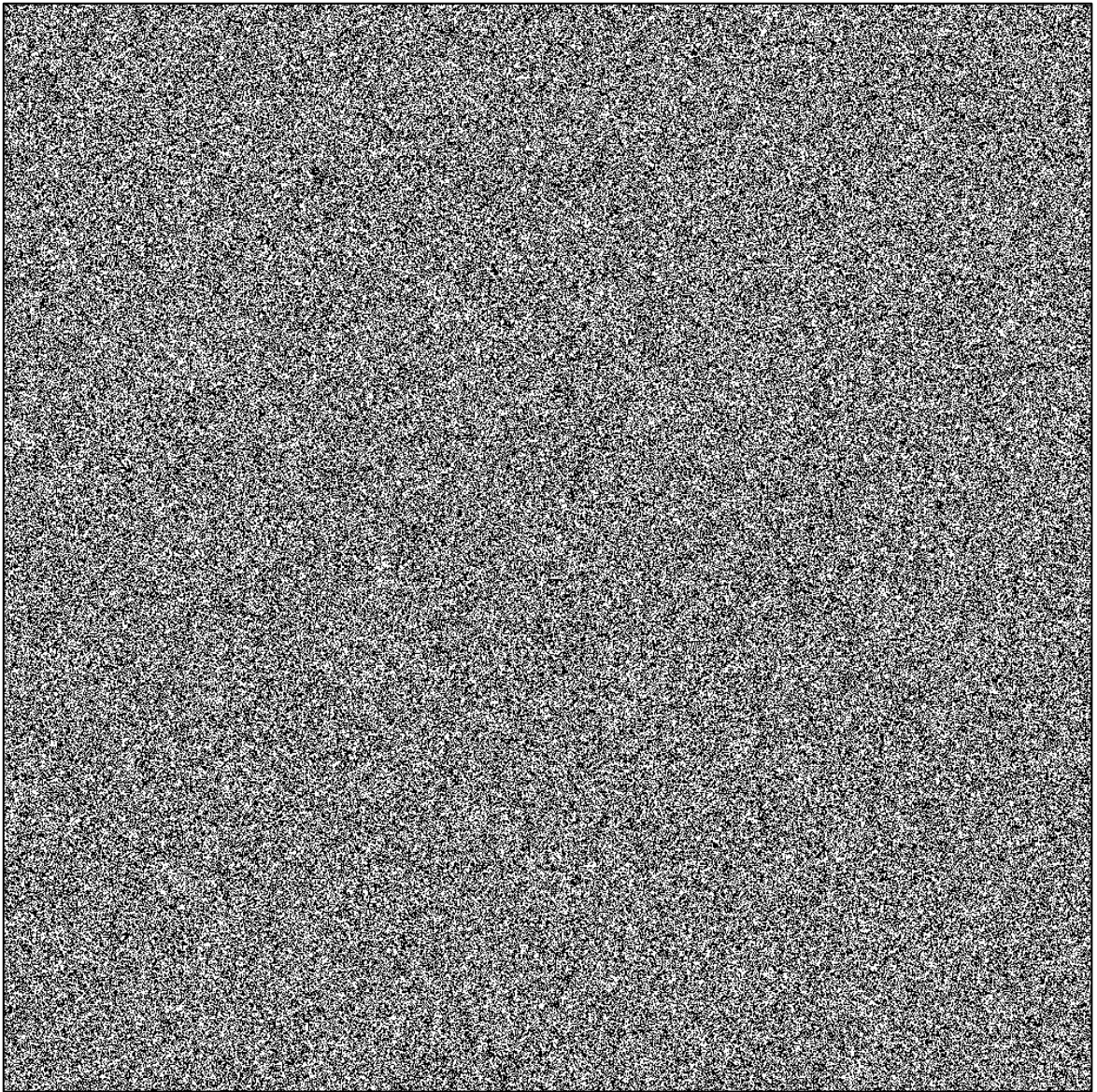


Figure 5.8. Image of the post-processed 1 million bits

## 6. CONCLUSION

### 6.1. WORK SUMMARY

A metastability-based TRNG was designed in 65-nm CMOS technology. This circuit operates with 100 MHz clock frequency and includes a post-processor inside it. The TRNG performs a random bit throughput of 12.5 Mbps, with a total power consumption of 375  $\mu$ W. The design is PVT-variation tolerant, achieves a high entropy with a single entropy source. The random bitstream passed all NIST tests with measured Shannon Entropy up to 0.99999886881164 under transient noise simulation. The energy efficiency was measured as 30 pJ/bit. The size of the layout excluding the output buffers is 75.565  $\mu$ m  $\times$  64.59  $\mu$ m.

### 6.2. COMPARISON WITH OTHER WORKS

This work is compared with other works in Table 6.1. The operating frequency of the metastability-based entropy source designed in 65-nm CMOS technology can be increased due to its capability for a higher data rate. However, a much slower clock frequency must be applied to the entire digital circuit blocks to operate simultaneously with the entropy source. Therefore, even if the entropy source is roughly designed in a similar way in newer CMOS process technologies, the remaining digital circuit block can be designed in a much smaller footprint, with a higher data rate, and with less power consumption. As a result, it seems clear that this work will be much more efficient when designed in newer CMOS process technologies.

Table 6.1. Comparison with other works

| Work              | [2]                  | [8]                 | [11]                 | [14]                 | [15]                 | This Work            |
|-------------------|----------------------|---------------------|----------------------|----------------------|----------------------|----------------------|
| Process           | 0.25- $\mu\text{m}$  | 40-nm               | 0.18- $\mu\text{m}$  | 45-nm                | 14-nm                | 65-nm                |
| Type              | Direct Amplification | Oscillator Based    | Chaotic Based        | Metastability Based  | Metastability Based  | Metastability Based  |
| Entropy           | Not declared         | Not declared        | Not declared         | 0.9999999993         | 0.9999999995         | 0.9999988688         |
| Throughput        | 2 Mbps               | 2 Mbps              | 35 Mbps              | 2.4 Gbps             | 162.5 Mbps           | 12.5 Mbps            |
| Power Consumption | 1.9 mW               | 46 $\mu\text{W}$    | 1.15 mW              | 7 mW                 | 1.5 mW               | 375 $\mu\text{W}$    |
| Energy Efficiency | 950 pJ/bit           | 23 pJ/bit           | 33 pJ/bit            | 2.92 pJ/bit          | 9.23 pJ/bit          | 30 pJ/bit            |
| Area              | 1200 $\mu\text{m}^2$ | 836 $\mu\text{m}^2$ | 3600 $\mu\text{m}^2$ | 4004 $\mu\text{m}^2$ | 1008 $\mu\text{m}^2$ | 4881 $\mu\text{m}^2$ |

## REFERENCES

1. Holleman J, Bridges S, Otis BP, Diorio C. A 3  $\mu$ W CMOS True Random Number Generator With Adaptive Floating-Gate Offset Cancellation. *IEEE Journal of Solid-State Circuits*. 2008 May; 43(5): 1324-1336.
2. Matsumoto M, Yasuda S, Ohba R, Ikegami K, Tanamoto T, Fujita S. 1200 $\mu$ m<sup>2</sup> Physical Random-Number Generators Based on SiN MOSFET for Secure Smart-Card Application. In *2008 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*; 2008: IEEE. p. 414-624.
3. Brederlow R, Prakash R, Paulus C, Thewes R. A Low-Power True Random Number Generator using Random Telegraph Noise of Single Oxide-Traps. In *2006 IEEE International Solid State Circuits Conference - Digest of Technical Papers*; 2006: IEEE. p. 1666-1675.
4. Petrie CS, Connelly JA. A Noise-Based IC Random Number Generator for Applications in Cryptography. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*. 2000 May; 47(5): 615-621.
5. Bucci M, Germani L, Luzzi R, Trifiletti A, Varanonuovo M. A High-Speed Oscillator-Based Truly Random Number Source for Cryptographic Applications on a Smart Card IC. *IEEE Transactions on Computers*. 2003 April; 52(4): 403-409.
6. Petrie CS, Connelly JA. Modeling and Simulation of Oscillator-Based Random Number Generators. In *1996 IEEE International Symposium on Circuits and Systems. Circuits and Systems Connecting the World. ISCAS 96*; 1996: IEEE. p. 324-327.
7. Yang K, Fick D, Henry MB, Lee Y, Blaauw D, Sylvester D. A 23Mb/s 23pJ/b Fully Synthesized True-Random-Number Generator in 28nm and 65nm CMOS. In *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*; 2014: IEEE. p. 280-281.

8. Yang K, Blaauw D, Sylvester D. An All-Digital Edge Racing True Random Number Generator Robust Against PVT Variations. *IEEE Journal of Solid-State Circuits*. 2016 April; 51(4): 1022-1031.
9. Zhou T, Yu M, Ye Y. A Pipelined Switched-Current Chaotic System for the High-Speed Truly Random Number Generation in Crypto Processor. In *19th International Conference on VLSI Design held jointly with 5th International Conference on Embedded Systems Design (VLSID'06)*; 2006: IEEE. p. 6 pp.-.
10. Pareschi F, Pareschi F, Rovatti R. Implementation and Testing of High-Speed CMOS True Random Number Generators Based on Chaotic Systems. *IEEE Transactions on Circuits and Systems I: Regular Papers*. 2010 December; 57(12): 3124-3137.
11. Cicek I, Pusane AE, Dundar G. An Integrated Dual Entropy Core True Random Number Generator. *IEEE Transactions on Circuits and Systems II: Express Briefs*. 2017 March; 64(3): 329-333.
12. Beirami A, Nejati H. A Framework for Investigating the Performance of Chaotic-Map Truly Random Number Generators. *IEEE Transactions on Circuits and Systems II: Express Briefs*. 2013 July; 60(7): 446-450.
13. Ergün S. Lessons Learnt from the Cryptanalysis of a Chaos Based Random Number Generator. In *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*; 2017 July: IEEE. p. 197-200.
14. Mathew SK, Srinivasan S, A.Anders M, Kaul H, K.Hsu S, Sheikh F, et al. 2.4 Gbps, 7 mW All-Digital PVT-Variation Tolerant True Random Number Generator for 45 nm CMOS High-Performance Microprocessors. *IEEE Journal of Solid-State Circuits*. 2012 November; 47(11): 2807-2821.
15. Mathew SK, Johnston D, Satpathy S, Suresh V, Newman P, Anders MA, et al.  $\mu$ RNG: A 300–950 mV, 323 Gbps/W All-Digital Full-Entropy True Random Number Generator in 14 nm FinFET CMOS. *IEEE Journal of Solid-State Circuits*. 2016 July; 51(7): 1695-1704.

16. Kinniment DJ, E.G.Chester. Design of an On-Chip Random Number Generator using Metastability. In *Proceedings of the 28th European Solid-State Circuits Conference*; 2002: IEEE. p. 595-598.
17. Mathew SK, Johnston D, Satpathy SK, inventors; Random Number Generator. *U.S. patent* US 2017/0090872 A1. 2017 March 30.
18. Kobayashi T, Nogami K, Shirotori T, Fujimoto Y. A Current-Controlled Latch Sense Amplifier and a Static Power-Saving Input Buffer for Low-Power Architecture. *IEEE Journal of Solid-State Circuits*. 1993 April; 28(4): 523-527.
19. Razavi B. The StrongARM Latch [A Circuit for All Seasons]. *IEEE Solid-State Circuits Magazine*. 2015; 7(2).
20. Rabuske T, Fernandes J. Noise-aware simulation-based sizing and optimization of clocked comparators. *Analog Integrated Circuits and Signal Processing*. 2014; 81(3): 723-728.
21. Nuzzo P, Bernardinis FD, Terreni P, Plas GVd. Noise Analysis of Regenerative Comparators for Reconfigurable ADC Architectures. *IEEE Transactions on Circuits and Systems I: Regular Papers*. 2008; 55(6): 1441-1454.
22. Shannon CE. A Mathematical Theory of Communication. *The Bell System Technical Journal*. 1948 July; 27(3): 379-423.
23. Parker RJ. Entropy Justification for Metastability Based Nondeterministic Random Bit Generator. In *2017 IEEE 2nd International Verification and Security Workshop (IVSW)*; 2017: IEEE. p. 25-30.
24. Ahmad N, Hasan R. Topology of 2 input subnanowatt XOR gate in 65nm CMOS technology. *IEEE-ICSE2012 Proc*. 2012;; 597-599.
25. Bassham L, Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, et al. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. 80022nd ed.: National Institute of Standards and Technology; 2010.

## APPENDIX A: POST-PROCESSING USING MATLAB

The work done by the Correlation Suppressor subcircuit can also be done by writing a MATLAB code which is shown in Algorithm A.1. This code provides a post-processing operation after reading the raw data and creating a text file consisting of the bitstream output.

Algorithm A.1. MATLAB Code of Post-Processing

```
clear; %Clear the Workspace

SISO_bit = 29; % Size of SISO Shift Register
PIPO_bit = 8; % Size of PIPO/SIPO Shift Register
clk_div = 64; % Clock Division Frequency Value

fileID = fopen('8M_bitstream.txt','r'); % Reading the raw bitstream
formatSpec = '%1d';
size_d = [1 Inf];
a = fscanf(fileID,formatSpec,size_d); % "a" represents the raw data
fclose(fileID);

n = length(a); % length of bitstream (raw data)

b = zeros(1,n+SISO_bit); % "b" represents the last bit of the SISO Shift Register
%%% length of b is shifted according to the size of the SISO Shift Register %%%

for(t = 1:n)
    if(a(t) == b(t)) % XOR operation of "a" and "b"
        xor_out(t) = 0; % "xor_out" represents the output of the XOR Gate
    else
        xor_out(t) = 1;
    end

    b(t+SISO_bit) = xor_out(t);
    %%%% b is updated with the feedback loop according to xor_out %%%%
end

for k = 1:PIPO_bit
    pipo(k,:) = downsample(b,clk_div,clk_div-SISO_bit+k-1);
    % downsample(data,sample rate,offset) % PIPO Shift Register samples the data %
end
%%% b is sampled with a sample rate of 64 (clk_div value) %%%
%%% First sampling is skipped by giving 64 bit offset (offset=+clk_div) %%%
%%% Since b is shifted 29 bits at the beginning, sampling offset is updated to
%%% 64-29 --> (offset=+clk_div-SISO_bit) %%%
```

```

%%% PIPO matrix is formed with sampling each 8 bits(k value) of data(b)    %%%
%%% Each sampling is done from 0th to (k-1)th bit of data, so
%%% the final ofset value is --> (offset+=clk_div-SISO_bit+(k-1))          %%%

bit = reshape(pipo,[1,length(pipo)*PIPO_bit]);
% 8 bit PIPO output is converted into a single bitstream (End of the post-processing) %

% Generating Correlation Suppressor Output File %
fileID1 = fopen('post_data.txt','w');
fprintf(fileID1,'%d',bit);
fclose(fileID1);

```

