On-chip ID Generation for Multi-node Implantable Devices

Chang Gao
B.Eng in Electronics(Hons)
University of Liverpool, 2015

Supervised by:
Dr. Timothy Constandinou

A Thesis submitted in fulfilment of requirements for the degree of
Master of Science
MSc Analogue and Digital Integrated Circuit Design
of Imperial College London

Department of Electrical and Electronic Engineering
Imperial College London
September 9, 2016

Abstract

Being an important topic for on-chip communications, the problem of identifications for microelectronic systems has been studied extensively in recent years. As a requirement, this project aims to design an on-chip ID generation system for multi-node implantable devices. The silicon physical unclonable function (PUF) is such a promising solution to on-chip ID generation. This thesis presents a novel PUF bit cell architecture based on sense amplifiers as well as a whole system composed of an array of 64 bit cells arranged in the manner of an 8×8 matrix and implemented in the 0.35 μ technology. The proposed bit cell design achieved an uniformity of 50.24% and the IDs produced by the system achieved high quality with a simulated uniqueness around 50.04%. Moreover, the proposed system achieved an energy consumption of 6.0 pJ per bit with parallel outputs and 17.3 pJ per bit with serial outputs.

Acknowledgment

First of all, I would like to thank my supervisor, Dr. Timothy Constandinou, for accepting me to do this project at the beginning and his supervision during over this academic year. I am very grateful for his insightful suggestions on my project and the recommendation for a relevant PhD position.

I also want to thank Dr. Yan Liu and Dr. Sara Ghoreishizadeh for their time spent on weekly meetings with me. They always provide feedbacks of my project progress rapidly and without their continuous supports on all of my questions about the project, I would not have been able to accomplished the proposed design.

Finally, I cannot be more grateful for the encouragement and unparalleled supports from my parents, my father Mr. Jinguang Gao and my mother Mrs. Xiufen Zheng. I also would like to express my gratitude to my girlfriend, Miss Tianqiong Du, for her care and company over the past year.

Contents

List of Figures

List of Tables

Abbreviations

ASIC:	Application-Specific Integrated Circuit
BR:	Bistable Ring
CMOS:	Complementary Metal-Oxide-Semiconductor
CRA:	Challenge-Response Authentication
CRP:	Challenge-Response Pair
DFF:	D-type Flip-Flop
FET:	Field-effect Transistor
GC:	Generation Controller
HD:	Hamming Distance
IC:	Integrated Circuit
ID:	Identification
I/O:	Input/Output
IP:	Intellectual Property
MOSFET:	Metal-Oxide-Semiconductor Field-Effect Transistor
MUX:	MUltipleXer
DEMUX:	DEMUltipleXer
NOR:	Not OR
NAND:	Not AND
NFET:	N-channel FET
PFET:	P-channel FET
PUF:	Physical Unclonable Function
RC:	Readout Controller

RFID:	Radio Frequency IDentification
RO:	Ring Oscillator
ROM:	Read-Only Memory
SA:	Sense Amplifier
SRAM:	Static Random-Access Memory

Chapter 1

Introduction

1.1 Motivation

IN many applications of integrated circuits (IC), on-chip unique identification (ID) is important for chip authentication. This is especially essential for a multi-node implantable device, which is typically composed of numerous slave nodes since communications between the master chip and slave nodes can be successfully established only if all nodes are appropriately addressed by individual IDs. Moreover, on-chip ID generation has applications in radio-frequency identification (RFID) for labelling tags, wireless sensors node addressing, cryptographic key generation and licensing for intellectual property (IP) protection. To realize all those applications, a system, which has the ability to generate IDs with high uniqueness, low cost, simplicity in implementation and high compatibility with various complementary metal-oxide-semiconductor (CMOS) processing technology, is crucial. For this purpose, the idea of using silicon physical unclonable functions (PUF) for on-chip ID generation has exist for a long time.

Although there are various existing PUF designs, not all of which are suitable for universal applications. As for this project, the required ID generation circuit is specially designed for multi-node biomedical implantable devices. In this case, desiderata of this specific circuit include not only the quality of generated IDs but also the ability to achieve ultra-low power consumption during runtime and low hardware complexity for small chip area.

This thesis presents a novel PUF structure, of which the design inspiration originates from the topology of a sense amplifier (SA). Moreover, the full-custom design of a 64-bit on-chip ID generation system, which possesses the ability to generate high quality IDs, is presented. The system is composed of a 8×8 bit array containing 64 bit cells based on the proposed PUF design as well as digital readout blocks. The circuit was implemented in 0.35 μ CMOS technology with 3.3 V power supply.

1.2 Objectives

Objectives of this project is described below:

1. To propose a PUF design that can produce IDs with high quality;
2. To complete a ID generation system with correct functionality and ultra-low power for the purpose of being used on implantable devices.

1.3 Thesis Organisation

Chapter 2 introduces basic concepts in the area of on-chip ID generation as well as histories and background knowledge of PUFs, such as the definition of Challenge-Response Authentication (CRA), concerns on the PUF security properties and criteria on how to measure the quality of a PUF design.

Chapter 3 reviews some previous work to describe details of some promising PUF designs to show insights of designing a PUF.

The proposed design of a sense amplifier based PUF (SA-PUF) is introduced in Chapter 4, of which the principle of random bit generation, the operation scheme, how a parasitic compensation is applied to the layout design and simulation results are discussed in detail.

Then the design of the system, using an SA-PUF array to produce unique IDs and having ability to read them out, is showcased in Chapter 5. Emphasis is paid on the specification of the system and how blocks cooperate to realize required functions. Simulation results are shown to characterise the performance of the system and the quality of generated IDs.

Chapter 6 gives a conclusion for the proposed work presented in this thesis. Limitations are discussed to show potentials of optimization and relevant future works are raised.

Chapter 2

Background

2.1 Introduction

IN recent years, diverse ID generation methods have been proposed by researchers. Before focusing on the deliverables of this work, in this chapter, concepts of silicon PUFs implemented in CMOS technology are described in detail as a preparation for the presentation of this work.

A PUF is a system usually implemented in conventional IC technologies that exploit physical disorder properties throughout the fabrication process for authentication purposes and is impossible to be reproduced in a replica. The emergence of predecessors of PUFs dates back to Bauder in 1983 [4], who proposed an early authentication system whose behaviour follows the aforementioned theory. The concept was later formalized and named the Physical One-Way Function by Ravikanth et al. [5] in 2001. In 2002, the notion of PUF was first described by Gassend, et al. [6], who suggested that a PUF can be a complex IC fabricated on silicon. In recent years, as a promising identification/authentication solution, the discussion of PUF is still ongoing and thus many competitive PUF architectures have been proposed. Quintessential models includes the delay PUF and the SRAM PUF, which are discussed later.

2.2 Principle of Silicon PUFs

As a promising way to create ”fingerprints” of silicon, silicon PUFs have advantages in low cost and compatibility with mature processing technologies, and thus have been paid considerable attentions by many scientists.

The virtual impossibility of being duplicated of CMOS PUFs originates from the erratic and factors intrinsically belonging to their physical entity, which is the microstructure of a piece of silicon. Some of those factors are introduced during the fabrication of circuits, such as mismatch of the size of transistors [7, 8], random dopant fluctuation [9, 10] and the variation of oxide thickness across the wafer, all of which exist irreversibly and induce differential performance of chips manufactured in the same process. Besides, the random variation of signal delays through wires and logic gates is another factor that can be exploited. Moreover, oxide breakdown is a method to create read-only-memory(ROM)-like circuits by deliberately breaking the oxide gates of transistor in order to provide randomness or to store IDs generated by other PUFs.

Various PUF structures utilize different part of those factors as sources of uncertainties to achieve randomness and uniqueness for the purpose of identification or authentication.

Noise is another factor that is able to provide high randomness, nevertheless, it is unreliable, causing unstable circuit behaviour and thus cannot be utilized for practical applications.

2.3 Challenge-Response Authentication (CRA)

As an authentication protocol, CRA is formulated so that authentication is warranted only if a valid answer is presented in respect to its corresponding input stimulus. The ”challenge” and the ”response” here receptively denotes the stimulus and the answer to it. A challenge and its valid response form a challenge-response-pair (CRP), which is used for identifying a specific entity.

PUFs utilize CRA to evaluate the identity of a specific microstructure. A challenge is in practice a physical stimuli on the microstructure, which can be seen as an input of the authentication system. The response denotes the reaction of the system and thus can be regarded as the output. Sophisticated interactions of challenges with the system provide uncontrollable and unpredictable mappings between challenges and responses so that a PUF is able to create unique CRPs for integrated circuits according to their differential physical microstructures.

2.4 Security Concerns of PUFs

According to the number of CRPs available and its rate of growth with the physical size, there are two types of PUFs, weak PUFs and strong PUFs [11]. A strong PUF is defined as possessing a large number of CRPs, which usually grows exponentially with the PUF size, such that the success rate of being attacked by exhaustion methods is negligible [12]. A weak PUF has a linear rate of growth of its amount of available CRPs and is vulnerable to many forms of attacks.

As for this work, the objective is to design a dedicated PUF for biomedical implantable devices so that the functionality focuses on identification with ultra-low power and small chip area. Strong PUFs spends much more chip area and energy and are beyond the scope of this work. In this case, the PUF proposed in this work has only one CRP for each chip sample, which is an extreme case for a weak PUF.

2.5 PUF Quality Metrics

Two important quality metrics of PUFs include the uniqueness and the reliability.

Uniqueness measures the identifiability of a PUF. The definition of the uniqueness for a given PUF design is the average normalized inter-class Hamming distances (HD) of responses to the same challenge set [2], which is given as

$$\frac{2}{m\,(m-1)}\sum_{u=1}^{m-1}\sum_{v=u-1}^{m}\frac{HD\,(R_u,R_v)}{n}\times 100\%, \tag{2.1}$$

where m denotes the number of independent chips having the same PUF design implemented on. u and v denote any pair of chips out of all possible pairs. n is the length of pair-wise binary response R_u and R_v in bits. For an PUF with ideal performance, the uniqueness equals to 50%, which indicates that the PUF has the highest ability to identify chips.

Reliability measures how stable the response is for the same set of challenge towards the same chip. It is defined by the average intra-class Hamming distance between responses, which are measured under different operating conditions, and the reference response, which is measured under the normal operating condition [2]. The formula for calculating the reliability is given as

$$\frac{1}{z}\sum_{x=1}^{z}\frac{HD\left(R_x,R'_{x,y}\right)}{n}\times 100\%, \tag{2.2}$$

where R_x is the reference response and $R'_{x,y}$ denotes responses measured for z times under varying operating conditions. In ideal case, reliability should be 0%, which indicates that the PUF can achieve the highest stability without making errors.

Chapter 3

Literature Review

3.1 Introduction

IN this chapter, some typical PUF structures are described based on their principle and whether they are appropriate to be used for the purpose of chip identification for multi-node biomedical implantable devices. Some thoughts of the author in respect to the pros and cons of each design are also discussed.

3.2 Delay Based PUFs

In general, the drift velocity of electrons in a piece of conductor is at Fermi velocity, of which the magnitude is typically smaller than the light speed. Moreover, the propagation speed of signals through logic gates is limited by the switching speed of MOSFETs. Delay based PUFs exploit the randomly varying delays to create randomly distributed CRPs. Typical examples of this type of PUFs include arbiter PUFs [1, 13] and ring oscillator PUFs (RO-PUF) [14, 15].

3.2.1 Arbiter PUFs

The arbiter PUF is a representative of delay PUFs. A typical architecture of this kind of PUF is shown below.

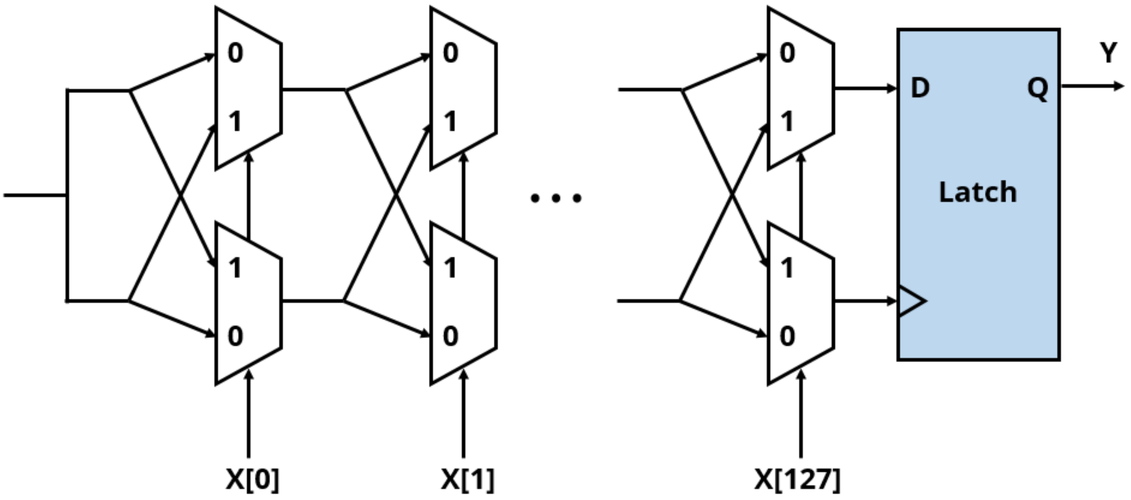


Figure 3.1: An arbiter PUF delay circuit (redrawn from Suh et al. [1])

Fig. 3.1 depicts the structure of an arbiter PUF based on two 128-stage chains of multiplexers (MUXes) and a latch behaving as an arbiter. The first stage shares one input and thus the circuit creates two paths for the input challenge signal to pass through. Both of the paths have the same total length of interconnections in a symmetrical layout. The direction of propagation of signals can be varied by changing the challenge X[0:127]. After a rising signal is introduced into both path simultaneously, the latch, of which the D terminal and clock input are respectively connected to the end of two signal paths, determines in which path the signal drifts faster and then generate a response Y [1]. As for the particular design illustrated in this figure, the output will be one if the signal in the path connected to terminal D of the latch is faster.

It has been claimed that the uniqueness of an arbiter PUF implemented on FPGA can be as low as 1.05% [16]. This is because the layout of arbiter PUF must be highly symmetrical to ensure the difference of path length is as small as possible to enhance the randomness of CRPs. In this case, the arbiter PUF is suitable to be integrated in an ASIC chip. However, since the number of transistors in a bit cell is large for an arbiter PUF, it spends large area to generate multi-bit IDs.

3.2.2 RO-PUFs

Another delay based PUF is RO-PUFs, whose block diagram is shown below. .

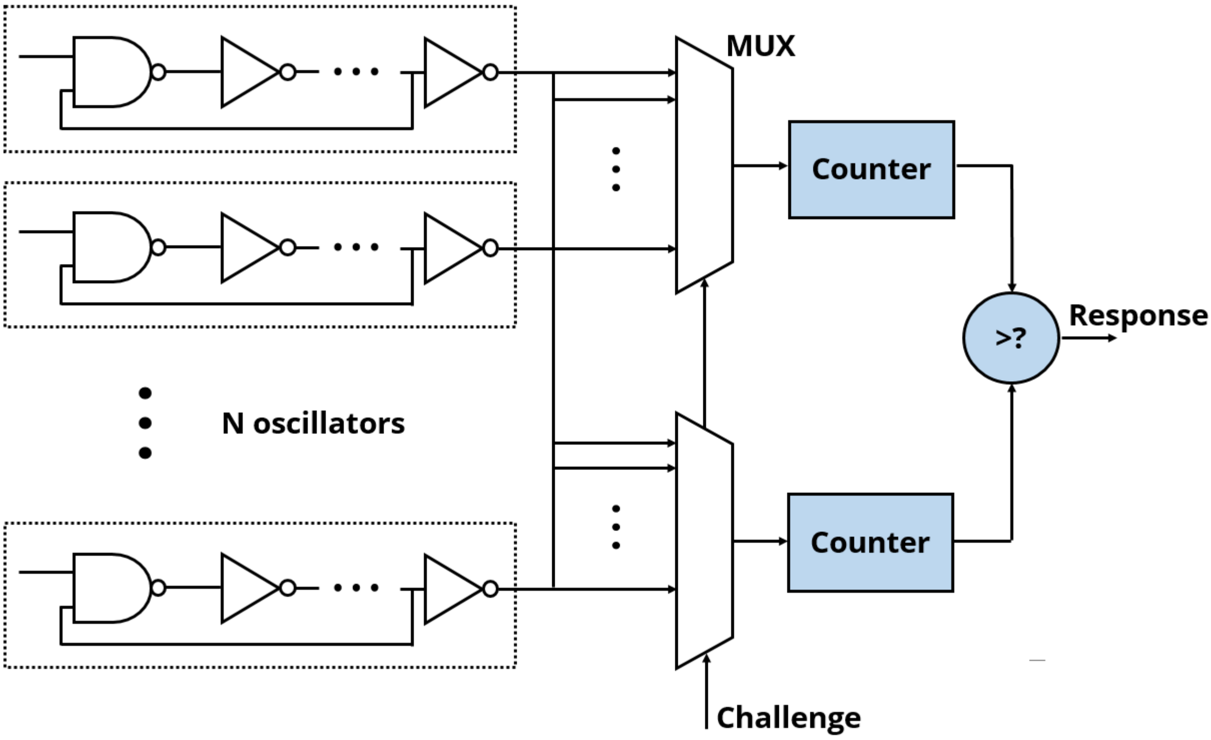


Figure 3.2: A RO-PUF circuit (redrawn from Suh et al. [1])

Fig. 3.2 illustrate how a RO-PUF is constituted. Ring oscillator is a circuit formed of odd numbers of cascaded delay units, such as inverters, connected in a close loop chain. It has no stable output state and oscillate at a particular frequency, which is ruled by the propagation delay of each delay unit as well as the amount of delay units [17]. Due to process variation in manufacturing, the propagation delay of gates cannot be predicted, which produces randomness.

To generate 1 bit response, the RO-PUF compares the frequencies of two out of N ring oscillators selected by using two MUXes. By simultaneously enabling the two counters driven by outputs of the two MUXes for a period of time, the outputs of the two counters finally represent the frequencies of the two selected ring oscillator. The challenge input determines which exact two oscillators are selected.

The RO-PUF has the similar problem in large bit cell area with the arbiter PUF. Furthermore, a large amount of dynamic power consumption is introduced due to oscillations.

3.3 The Bistable Ring PUF (BR-PUF)

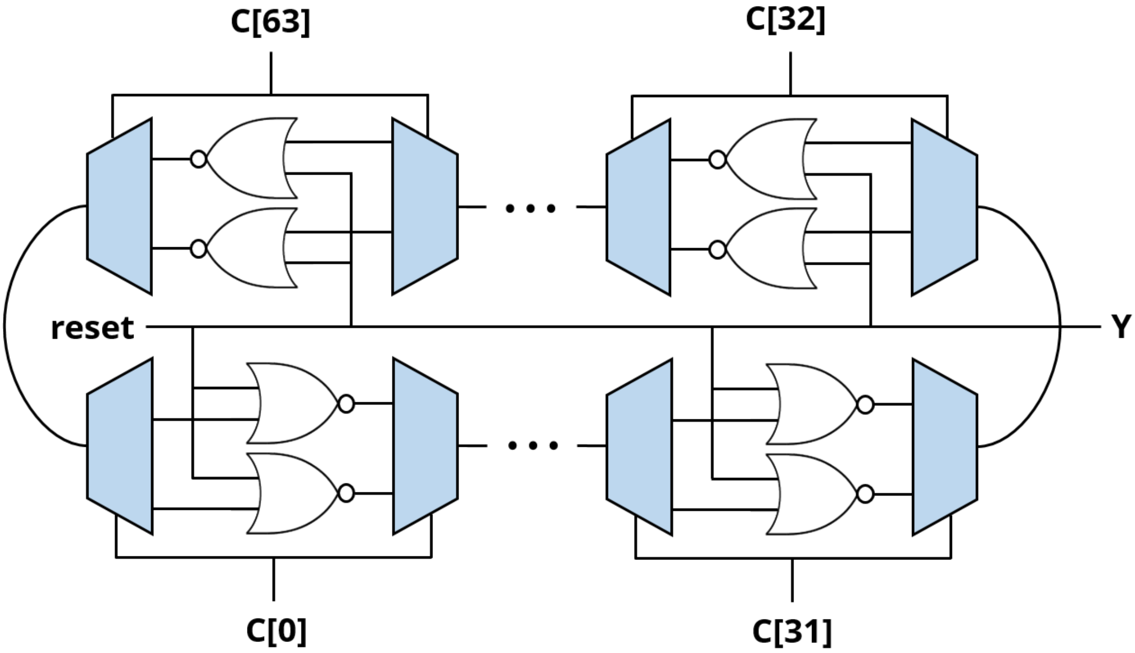


Figure 3.3: A bistable ring PUF Circuit (redrawn from Chen et al. [2])

In 2011, Chen et al. [2] suggested a novel PUF architecture called BR-PUF, which is shown in Fig 3.3. It has a closed loop composed of even numbers of NOR/NAND gates so that there are two possible states for the loop to be stable at. This phenomenon is utilized to generate random CRPs.

Furthermore, each stage of the loop is designed to have two NOR/NAND gates. MUXes and DEMUXes are inserted between each stage to select one of the two NOR/-

NAND gates to be connected in the loop. In this case, the number of CRPs has an exponential growth rate against the total number of NOR/NAND gate stages, making BR a feasible architecture to establish a strong PUF.

3.4 SRAM PUF

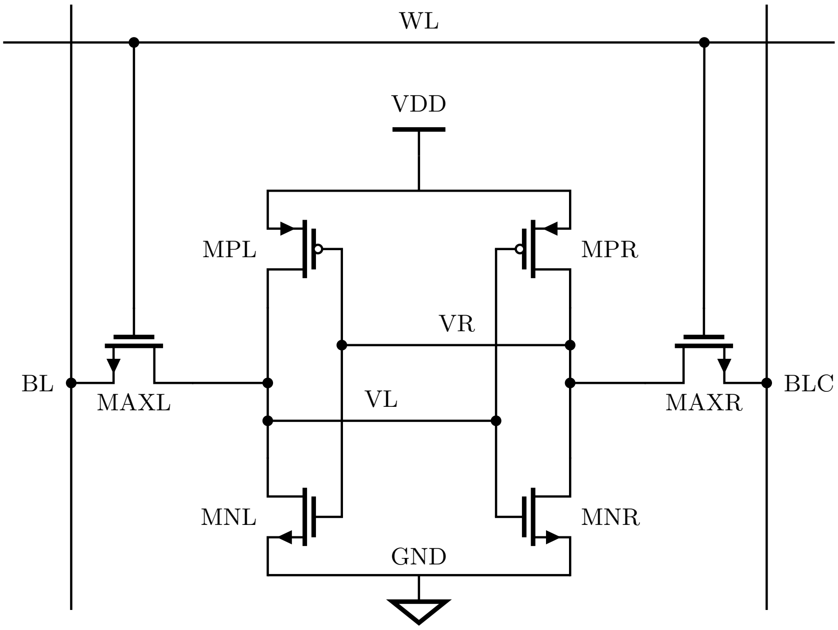


Figure 3.4: Structure of a six transistor SRAM cell.

Fig. 3.4 shows the circuit of a SRAM cell composed of six transistors. The four inner transistors (MPL, MPR, MNL, MNR) forms two cross-coupled inverters which can store 1-bit value. Bit lines (BL, BLC) are connected to two access transistors (MAXL, MAXR) which is controlled by the write line (WL).

As a digital component, SRAM cells are usually fabricated by using smallest scale transistors in a process technology, thus making it vulnerable to any intrinsic fluctuation at the atomic level [18], such as microscopic variation of the dopant concentration in the MOSFET channel region which influence the value of the threshold voltage [10]. During power-up or start-up, any difference of voltage VL and VR due to intrinsic process variations will cause the SRAM cell output to be 1 or 0. Since the variation is unpredictable and uncontrollable for transistors, different SRAM cells should have independent electrical behaviours.

Moreover, there has been researchers finding that once being implemented on a chip, SRAM cells have high probability to produce the same output state at each start-up [19]. It means that for single SRAM cell, its output bit value does not change after being powered off and restarted, though there is a small fraction of cells having unstable output states. By combining a large number of SRAM cells, multi-bit ID can be generated from their random outputs.

3.5 Sense Amplifier Based PUF (SA-PUF)

As a critical circuit for the readout of SRAMs, sense amplifiers (SAs) amplify any minor voltage difference between two bit lines with large parasitic capacitance. By connecting the same input voltages at two inputs of a sense amplifier, it is expected to produce 1 or 0 with equal possibilities.

SA-PUF is rarely seen in publications excluding the one proposed by Bhargava et al. [27] in 2010. This work will be compared to the proposed work in terms of performance at the end of Chapter 5.

3.6 Other ID Generation Methods

3.6.1 Antenna Effect

During the plasma processing in MOSFET fabrication, a thin oxide layer under a gate which is only driven by a large piece of top layer metal will occasionally suffer to plasma-induced charge damage [20, 21]. This phenomenon happens when excessive amount of charge is accumulated on the gate and is called the antenna effect [22].

A work proposed by Tang et al. [3] using antenna effect is illustrated in Fig. 3.5. The bit cell circuit is formed by two pull-up PFETs (MP2, MP4) and two NFETs (MN2, MN3) whose gates are connected together to the ground, which is also denoted as node AE. This node is where the antenna effect being applied on.

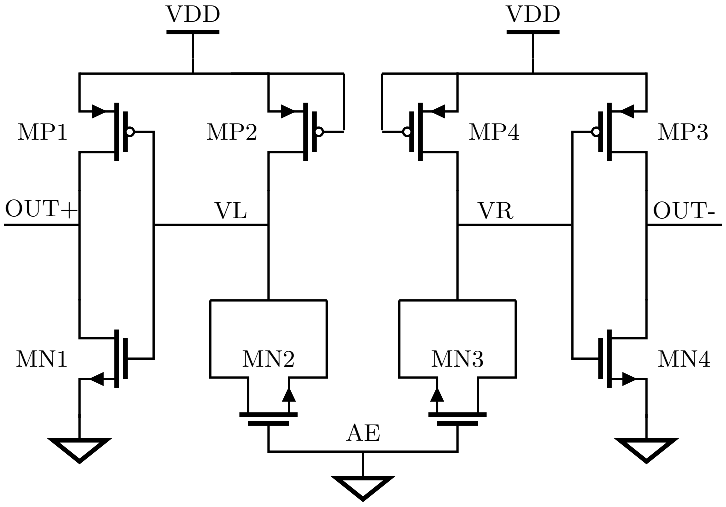


Figure 3.5: Schematic of a bit cell exploiting antenna effect (redrawn from Tang et al. [3])

By connecting node AE to a large area of top layer metal, the gates of MN2 and MN3 have possibilities to be broken down during the plasma process. Once the gate of any one out of two NFETs is damaged, the accumulated charge on node AE will be released through the diffusion region to the pull-up device connect to this NFET thus it guarantees that the gate of the other NFET keeps flawless. After the completion of top layer metal deposition, a voltage difference between node VL and VR is generated after connecting the top layer metal to the ground. Since the possibility for the two gates to be broken is regarded to be the same if the layout is symmetrical, by connecting two inverter at nodes VL and VR as buffers, the bit cell is able to produce complementary binary outputs to be used for on-chip ID generation.

The biggest advantage of this approach is its permanent reliability. Meantime, the problem of this design might be that there exist a third condition, in which neither of the two NFET gates are broken down. In this case, possible output states include: {0,1}, (0 for **OUT+**, 1 for **OUT-**), {1, 0} and {0,0}. If using the output of terminal **OUT+** as the reference, the existence of state {0,0} lead to unequal possibility of bit generation between 0 and 1. To compensate for it, the antenna metal has to be designed as large as possible to ensure that at least one of the two gates is broken down; however, it may spend more chip area. Moreover, once a gate is broken down, a static current path though the pull-up PFET channel and broken gate appears, which may increase the static power, though very low energy consumption at 1.2 pJ/bit was achieved by this work [3].

3.6.2 Oxide Breakdown

In 2010, Liu el al. presented a design called OxID [23]. It is composed of a memory array in which each cell contains a MOS capacitor with thin oxide as a fuse. During the generation process, each oxide layer is exposed to a stress voltage of 4.4 V, which is higher than the circuit power supply (VDD) of 1.1 V, for an identical length of stress time. Due to the uncontrollable variation of oxide thickness across the wafer, the length of time required for breaking a gate is unpredictable. Thus, at the end of the stress time, the distribution of broken gates should be random.

This method has the same advantage as the one using antenna effect, which is the permanent reliability provided that the gates have been completely broken down. According to [24], if the stress voltage does not reach the critical value, the oxide layer will be lead to soft breakdown, which does not completely change the functionality of the original circuits. Thus, the difficulty of this design is how to determine the critical voltage value.

Chapter 4

SA-PUF Bit Cell Design

4.1 Proposed Topology

THE design inspiration of the SA-PUF bit cell originates from a normal SA, which generates binary outputs by amplifying the tiny magnitude difference of input voltages of two bit lines.

Fig. 4.1 illustrates the proposed structure of the bit cell. Two pre-charge PFETs, **MP3** and **MP4**, of which gates are controlled by signal **TRIG**, are connected in parallel respectively with the two PFETs (**MP1**, **MP2**) of the SA. The output nodes **VL** and **VR** are connected to two access NFETs, of which gates are under the control of signal **EN**. Under the SA, two branches of current sources are respectively connected to the source of **MN1**, **MN2**. Each branch is composed of four NFETs in parallel, and all gates are directly connected to the power supply **VDD** of 3.3 V. Moreover, two NFETs (**MN3**, **MN4**) acting as switches are added to avoid direct connection between **VL**, **VR** and the two current sources branch in order to limit the contention current during the switching of signal **TRIG**.

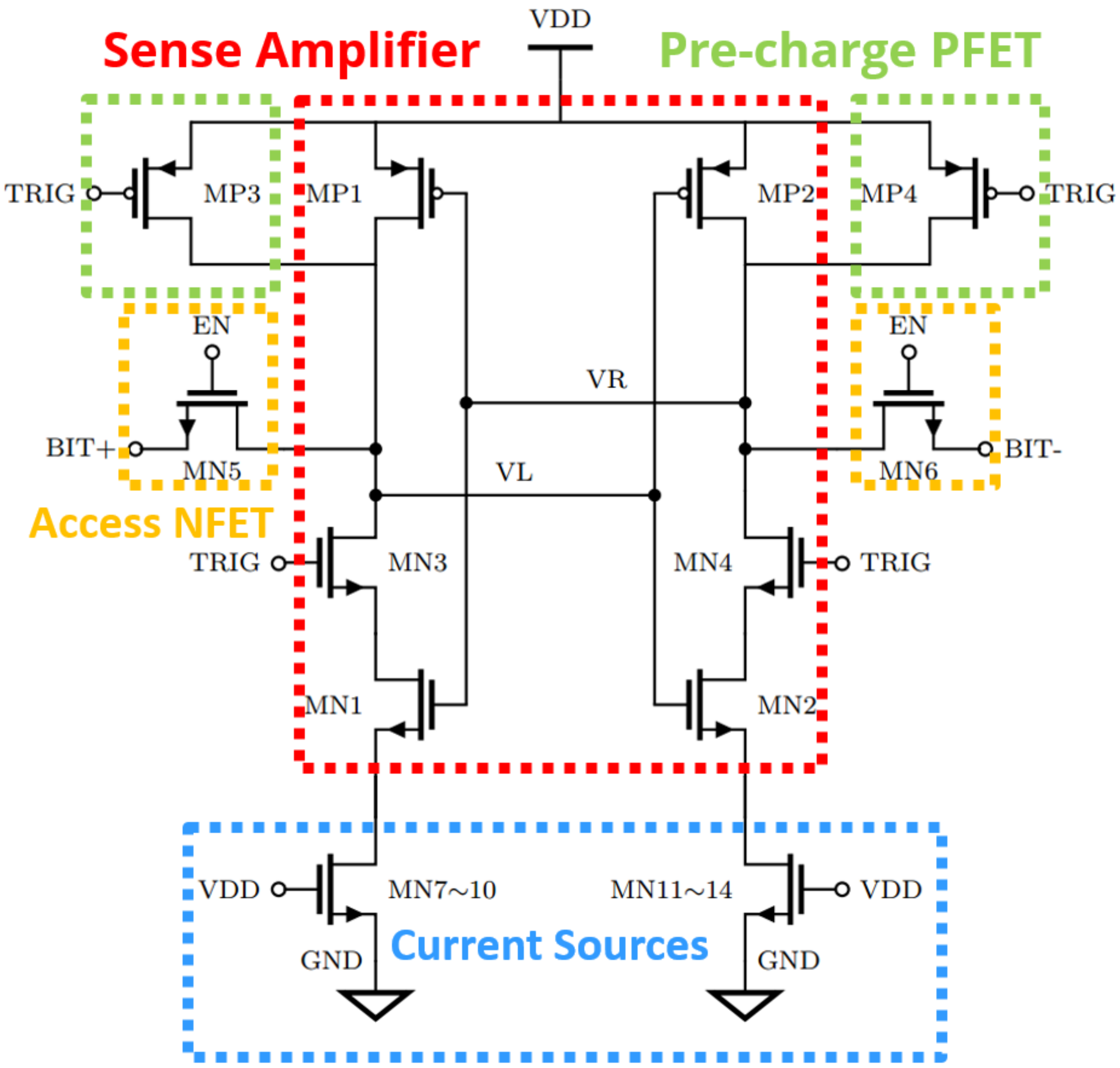


Figure 4.1: Circuit of the proposed sense amplifier based PUF bit cell

The principle of bit generation is to compare the difference of currents sinking into the two current source branches. Each branch contains four minimum sized transistors to strengthen the effect of mismatch between current sources on each side. The other transistors of the bit cell are all sized much larger than current source elements to reduce the effect of mismatch as much as possible. By doing this, the polarity of the bit cell is expected to be ruled by the mismatch of the current sources.

4.2 Bit Generation Scheme

The procedure of producing an ID bit follows the listed three steps:

1. **Pre-charge**: After the power-up of the cell, **TRIG** is first set to 0 to enable the two pre-charge PFETs so that nodes **VL** and **VR** are charged and the voltage of both nodes are raised to **VDD**;

2. **Generation: TRIG** is then set to 1 to switch off the two pre-charge PFETs. After that, nodes **VL** and **VR** start to discharge simultaneously. Any tiny difference of current between the two branches of current sources will leads to a final steady state {0, 1} (0 for **BIT+**, 1 for **BIT-**) or {1, 0}.

3. **Readout:** After the bit cell reach a steady state, **EN** is set to 1 to transfer the output values of the SA to bit lines.

4.3 Uniformity Concerns

For an ideal bit cell, the polarity should be 0 in order to have the same possibility of generating 0 or 1. This is measured by the metric called "uniformity", which is defined as

$$\frac{1}{k}\sum_{i=1}^{k-1} R_i \times 100\%, \tag{4.1}$$

where R_i denotes the value of the $i^t h$ binary response and k is the total time of execution of the bit generation scheme, which is clarified in the next section.

To achieve a bit cell with high uniformity, the layout must as symmetrical as possible. This is because polarity of the bit cell is also related to the total equivalent capacitance at nodes **VL** and **VR** in accordance with the following formula

$$i = C\frac{dV}{dt}. \tag{4.2}$$

Fig. 4.2 shows the equivalent circuit of the bit cell during the **Generation** state.

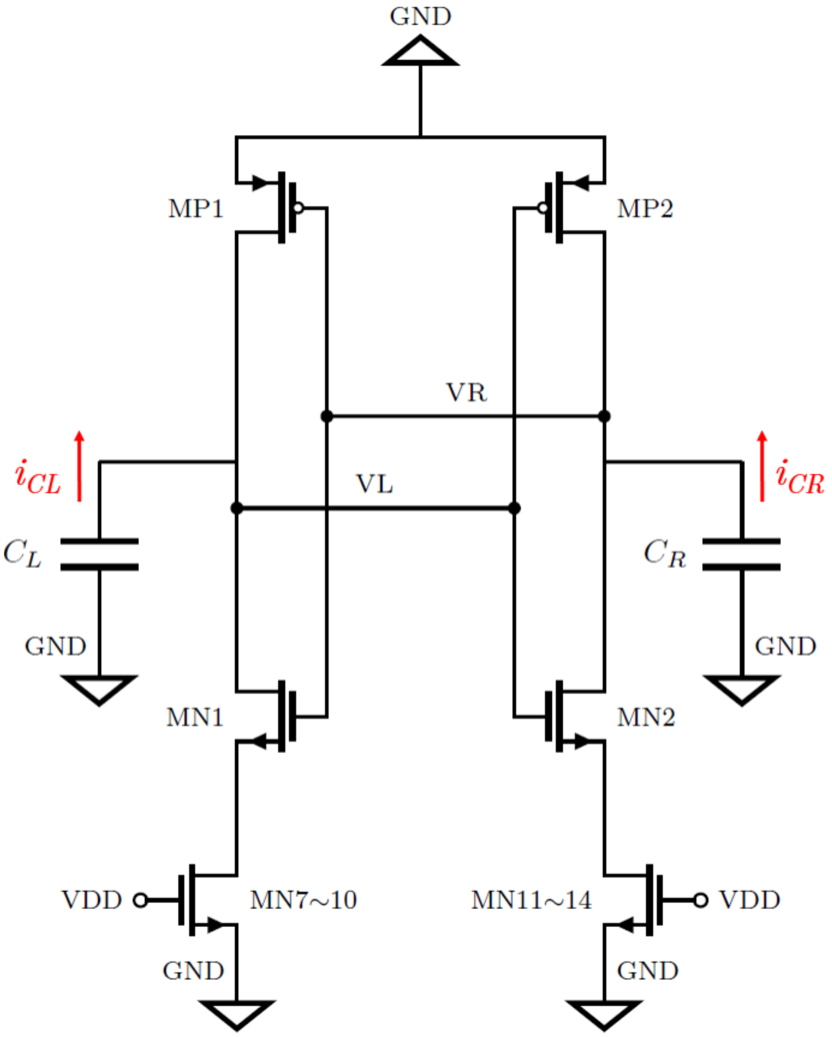


Figure 4.2: Small signal equivalent circuit of the bit cell in Generation state

The pre-charge PFETs and the access NFETs are removed due to being switched off. Since the two switches are turned on, channels of **MN3** and **MN4** are shorted by wires. C_L and C_R are respectively the total equivalent parasitic capacitance at nodes **VL** and **VR**. According to Eq. 4.2, assuming that the rate of change of voltage across C_L and C_R are the same at the beginning of **Generation**, the two induced currents i_{CL} and i_{CR} are respectively proportional to the magnitude of capacitance of C_L and C_R. In this case, the inequality of the capacitance of C_L and C_R will result in a difference between i_{CL} and i_{CR}, which induces an polarity of the bit cell.

4.4 Layout Design

Fig. 4.3 exhibits the layout design of the proposed bit cell.

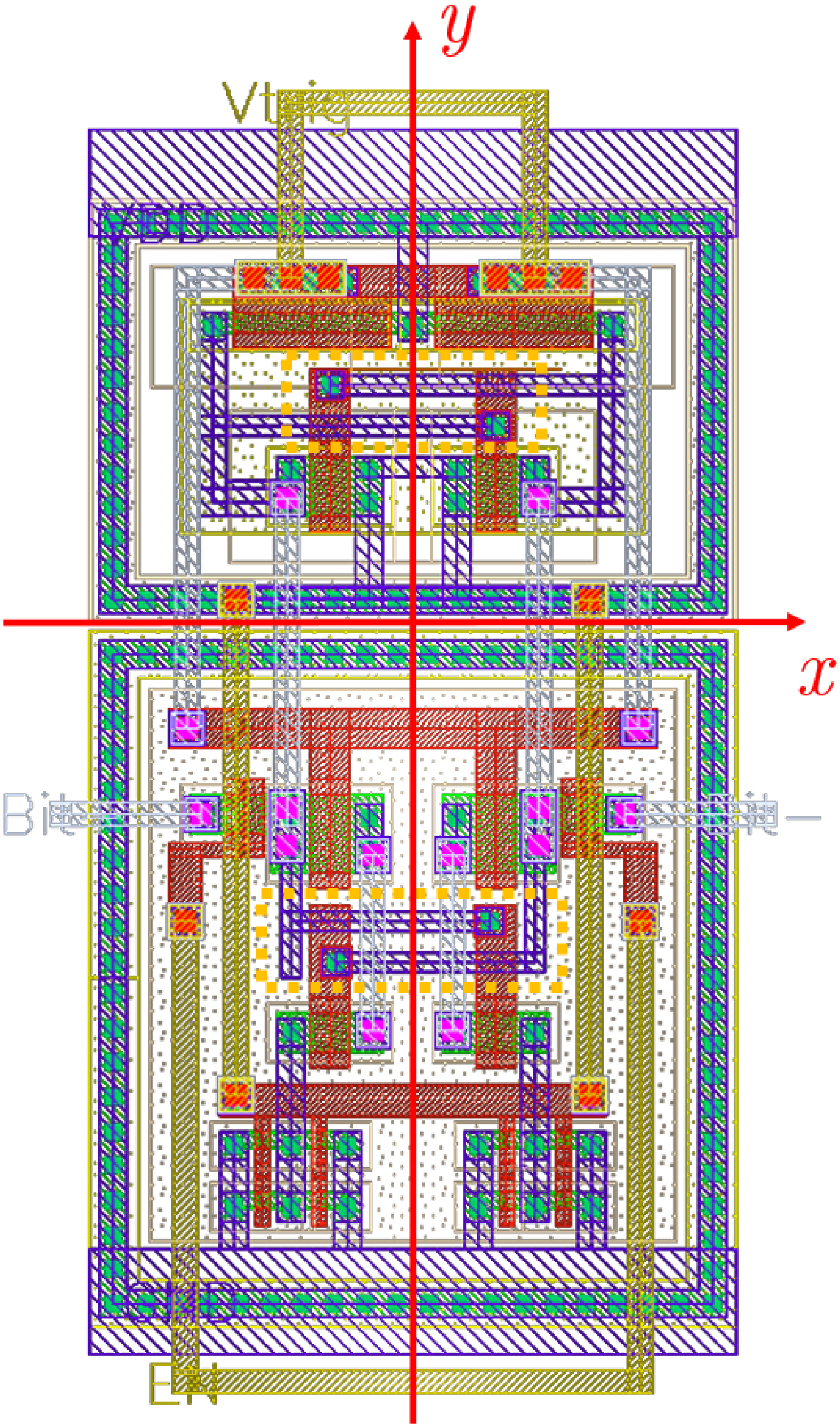


Figure 4.3: Circuit of the proposed sense amplifier based PUF bit cell

As shown in Fig. 4.3, the layout is designed to be highly symmetrical with respect to the y-axis. However, in the two regions each surrounded by a dashed box, the two cross-wired parts inevitably affect the symmetry of the layout. To compensate for it, a small amount of metal is added to the left side interconnections to make the post layout extraction results show equal parasitic capacitance at nodes **VL** and **VR**. Moreover, to isolate the bit cell from the interference of adjacent circuits and noise, guard rings are created for both PFETs and NFETs.

4.5 Simulation Results & Discussion

4.5.1 Timing of Bit Cell

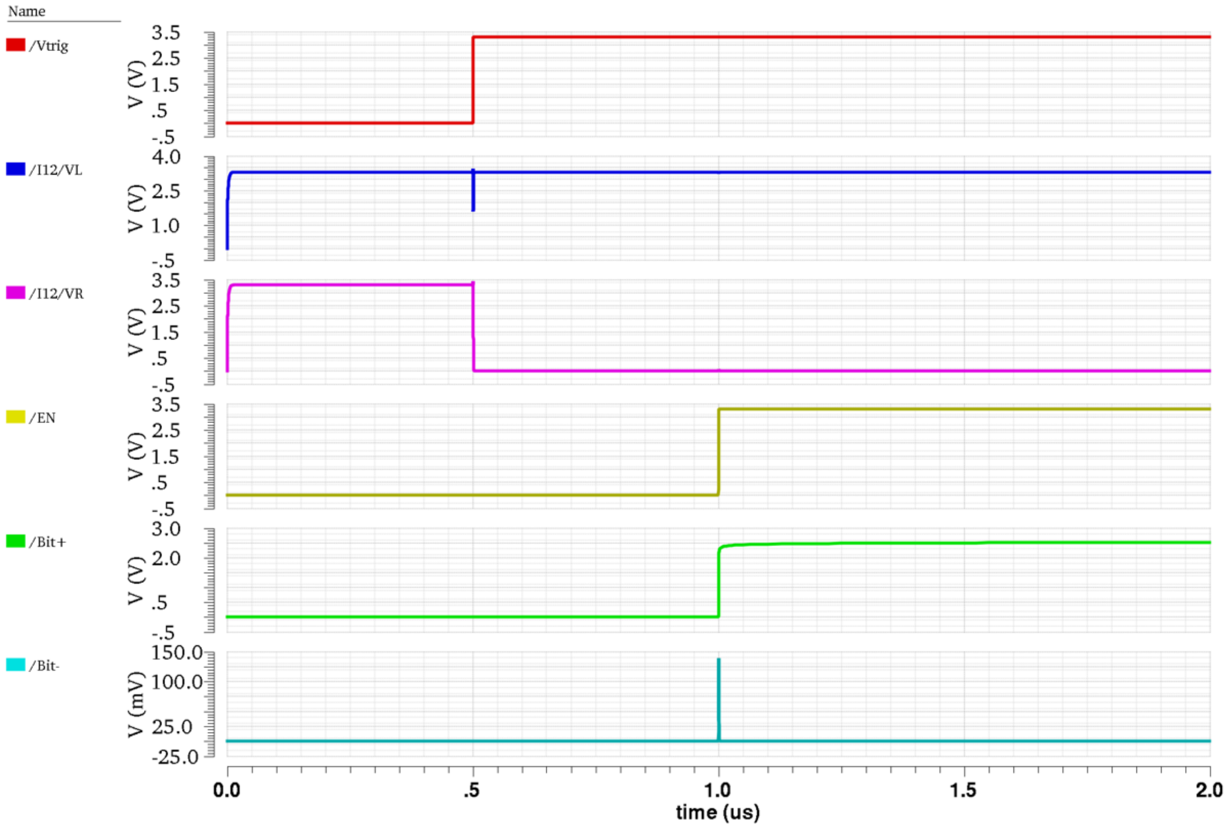


Figure 4.4: Transient simulation results of the bit cell

Transient simulation results in Fig. 4.4 illustrates the timing of the bit cell generation and read out. At the beginning of the simulation when **VTRIG** is set to 0 V, both nodes **VL** and **VR** are raised to 3.3 V. After **VTRIG** being switched to 3.3 V, due the aforementioned bit generation principle, the voltage at **VL** is still 3.3 V but the voltage at **VR** becomes 0 V. Finally, by raising **EN** to 3.3 V to switch on the two access NFETs, the results are available at output terminals **BIT+** and **BIT-**.

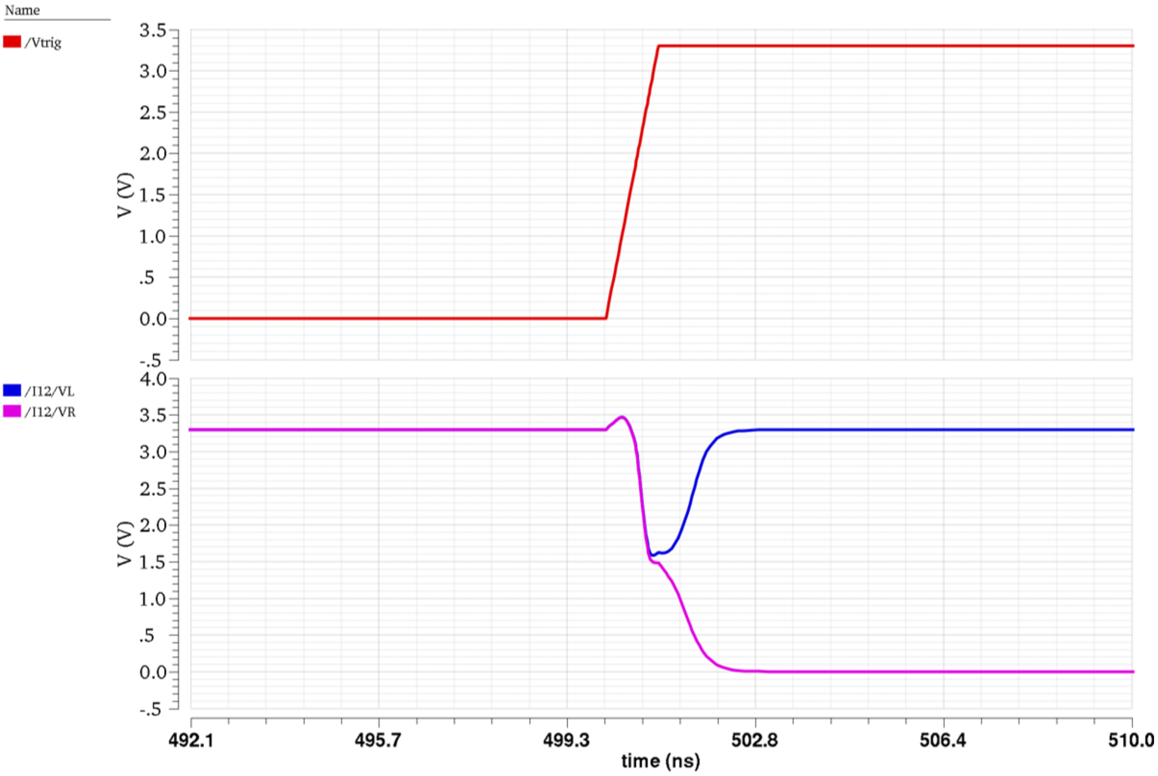


Figure 4.5: Transient simulation results of the bit cell (zoomed in)

Fig. 4.5 shows how the **VL** and **VR** changes during the pull-up of **VTRIG**. Two nodes starts to be discharged when **VTRIG** increases. It can be seen from the curve of **VL** and **VR** that the rate of descent of the voltage at **VL** is smaller than that of **VR**, which indicates that the current source connected to **VL** is relatively weaker due to the mismatch. As a consequence, **VL** goes up to 3.3 V again due to its slower discharging rate.

4.5.2 Bit Cell Uniformity

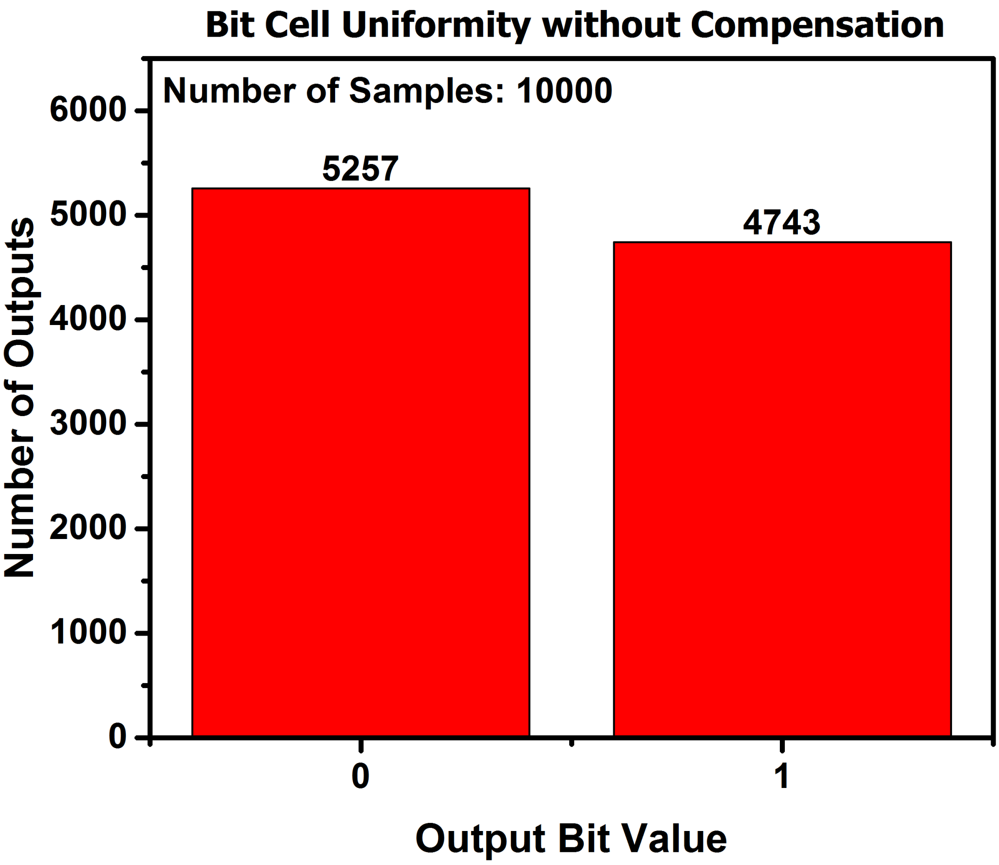


Figure 4.6: Results of Monte Carlo simulation of 10000 samples on a Bit Cell for the evaluation of uniformity (without layout compensation)

The uniformity of a **Bit Cell** represents how random the generated bit is. Fig 4.6 showcases the Monte Carlo simulation results of uniformity for a Bit Cell without compensation of parasitic capacitance on the layout design. In this case, the resultant uniformity is 47.43%, which indicates that the possibility of producing a 1 is slightly lower than producing a 0. Furthermore, by adding extra area of metal to the terminal, which generates more 0s than 1s, the resultant output distribution of the compensated **Bit Cell** is shown in Fig. Fig:bcuniformc. The optimized uniformity reaches 50.24%, which is much closer to the ideal value 50% than the uncompensated one.

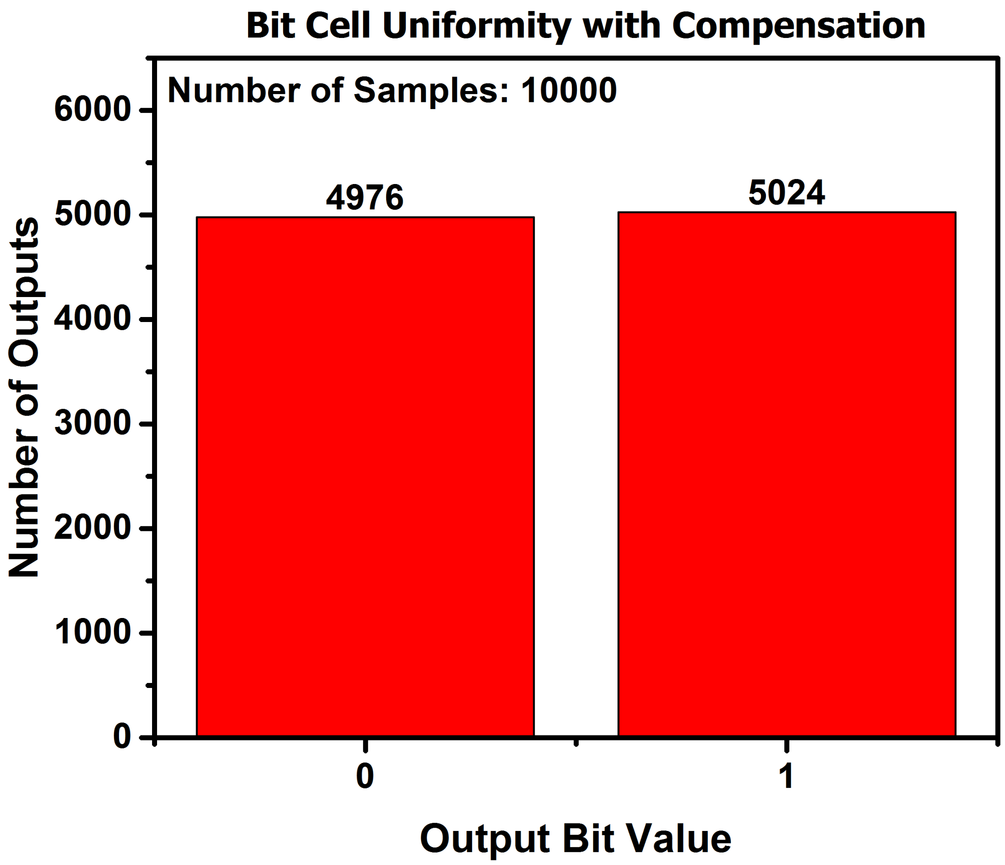


Figure 4.7: Results of Monte Carlo simulation of 10000 samples on a Bit Cell for the evaluation of uniformity (with layout compensation)

4.5.3 Robustness of Bit Cells with Temperature Variation

Fig. 4.8 shows the polarity changes with respect to temperature variations and the reference temperature is set to be 28°.

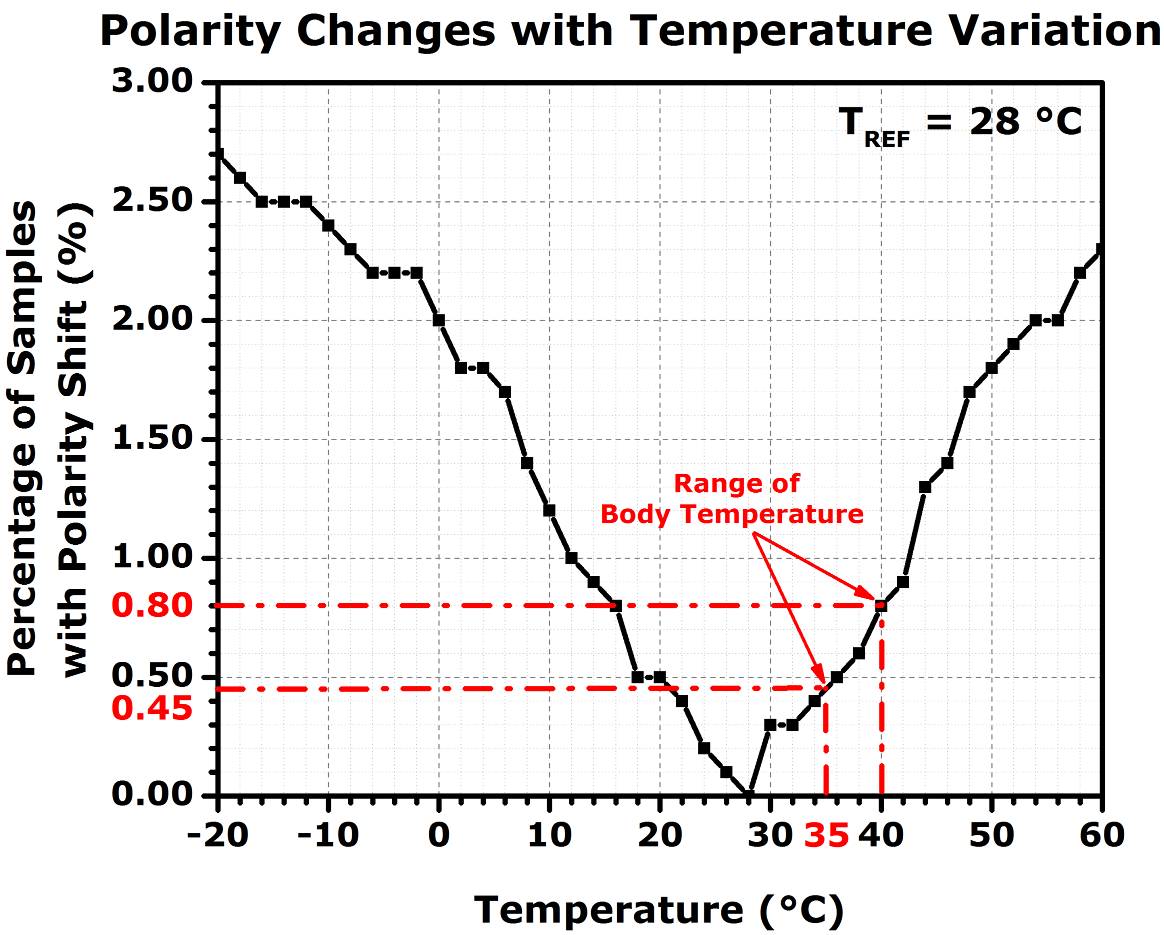


Figure 4.8: Polarity changes with respect to the variation of temperature by conducting Monte Carlo simulation with 1000 bit cells samples at each temperature point

The results are conducted by executing Monte Carlo simulations of 1000 samples at each temperature from -20° to 60°. It means that, at each temperature the same bit cell sample is restarted for 1000 times to evaluate the its ID generation outputs, which are expected to be all the same. Any occurrence of different outputs are denoted as a polarity change. As shown in the figure, the percentage of samples with polarity shift, within the range of human body temperature (35° [25] ~ 40° [26]), is from 0.45% to 0.80%. In this case, if the chip embedded with **Bit Cells** is implanted into a human body, the polarity shift rate with respect to 37.5°, which is the midpoint of the body temperature range, is around ±0.175%.

4.5.4 Robustness of Bit Cells with Supply Variation

Fig. 4.9 depicts the polarity changes with respect to supply voltage variations and the reference supply voltage is set to be 3.3 V°.

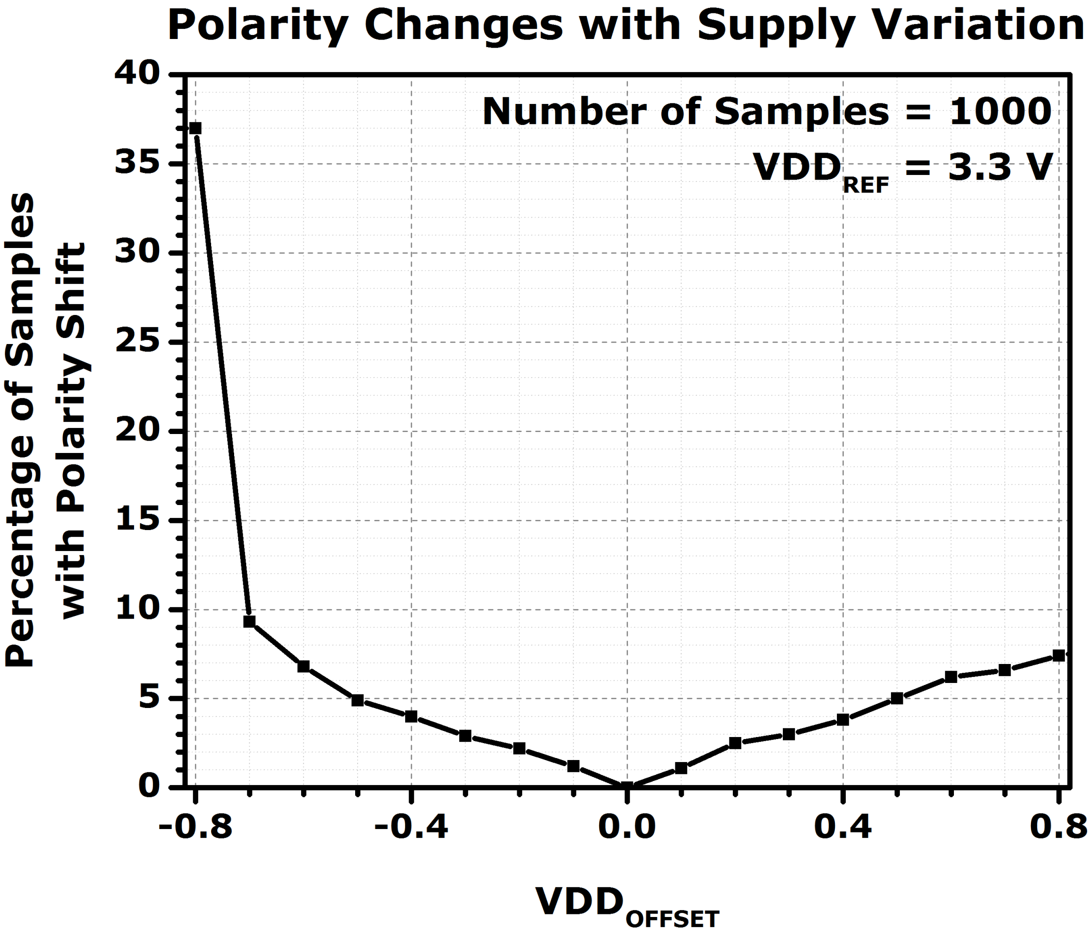


Figure 4.9: Polarity changes with respect to the variation of supply voltage VDD_{OFFSET} obtained in a Monte Carlo simulation on 1000 bit cells samples at 28°C.

Differing with the simulation on temperature variation, this one executes Monte Carlo simulations at each supply voltage with 1000 samples. According to results, the maximum polarity shift rate within a ±21% supply voltage deviation is 9.3% at VDD = 2.6 V (VDD$_{OFFSET}$ = -0.7 V). When the supply voltage is less than this magnitude, the functionality of bit cells is dead.

Chapter 5

ID Generation System Design

5.1 Overview

SINCE the principle and structure of the proposed SA-PUF bit cell has been illustrated, this chapter discusses the design of each blocks and how they are integrated into a whole system with the ability to generate IDs and read them out.

5.1.1 System Architecture

According to the functionality of blocks, the system is split into two parts, a **Generation** part and a **Readout** part. This is illustrated in the block diagram of the whole system shown in Fig. 5.1, while the schematic of the whole system is shown in Fig. A.1.

Generation Part

The **Generation** part is formed by a **64-Bit Array**, a buffer array called the **Trigger** and an FSM called **Generation Controller**.

The core of the system is the **64-Bit Array** containing 64 Bit Cells arranged in a 8×8 matrix style, which is the largest block of the system. It is surrounded by dummy cells along the perimeter to be protected from ambient interference and to enhance the symmetry of the block. The **Trigger** is controlled by the **Generation Controller** to provide the signal **TRIG**, which is connected to gates of pre-charge PFETs of all **Bit**

Cells.

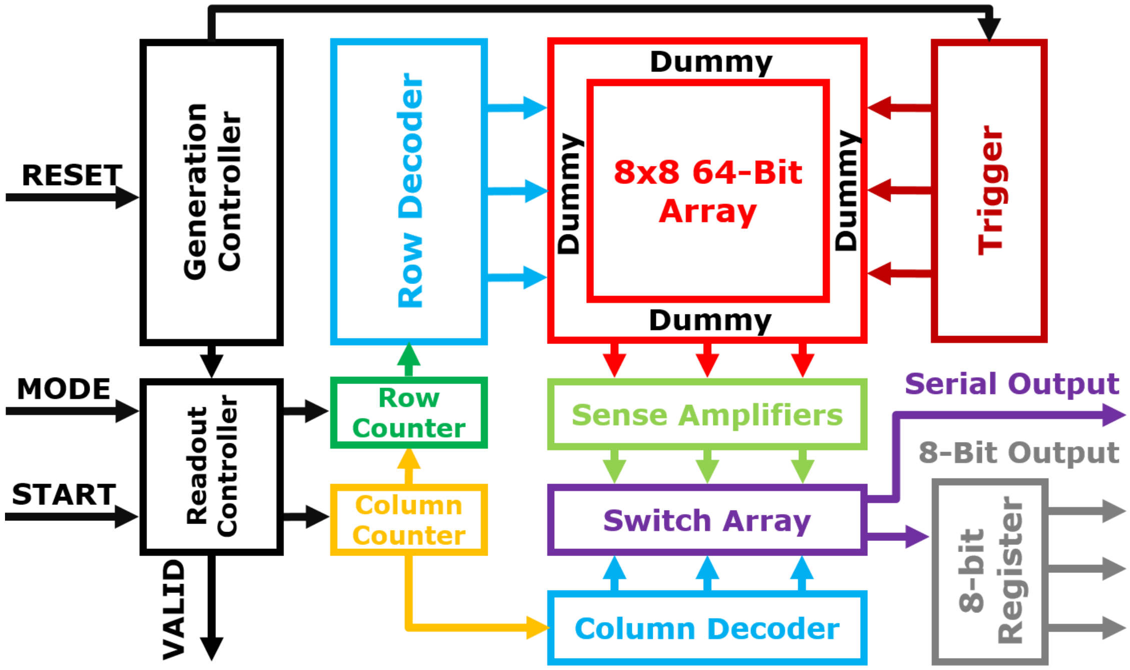


Figure 5.1: Block diagram of the proposed ID generation system

Readout Part

All rest blocks belong to the readout part, in which the **Readout Controller** controls the collaboration between blocks and the timing of input and output signals. Two pairs of counter and decoder are respectively responsible for providing a row index and a column index for each generated bit in the array. 8 sense amplifiers formed an array for amplifying the minor voltage swing in bit lines and their complementary outputs are connected to the **Switch Array** to be divided into the **Serial Output** and the **8-Bit Output**. Each output port is finally synchronized by using a specially designed low power D-type Flip-Flop.

5.1.2 Input/Output (I/O)

I/O ports of the system with their purposes are listed in Table 5.1.

Table 5.1: ID Generation System I/O ports

	Name	**Purpose**
Inputs	CLK	Clock signal
	RESET	Active low. Resetting the system.
	MODE	0 for Serial Output and 1 for 8-Bit Output.
	START	Active high. Starting the readout process.
Outputs	SOUT	Serial ID output
	POUT	8-Bit Parallel ID output
	VALID_SOUT	Active high. Asserted when SOUT is valid.
	VALID_POUT	Active high. Asserted when POUT is valid.

The behaviour of ID output ports of this system follows the so call "valid protocol", which means that the receiver of ID should be always ready for receiving the output IDs, **SOUT** or **POUT**, once the corresponding valid signals, **VALID_SOUT** or **VALID_POUT**, are active.

The input controlling signal **START** follows the "valid-enable" protocol. It means that ID requesters stall any request once the enable signal is inactive. In this scenario, **VALID_SOUT** and **VALID_POUT** are used for realizing the function of both "valid" and "enable" signal.

5.2 Block Analysis

5.2.1 64-Bit Array

Fig. 5.2 depicts the arrangement of bit cells in the bit array.

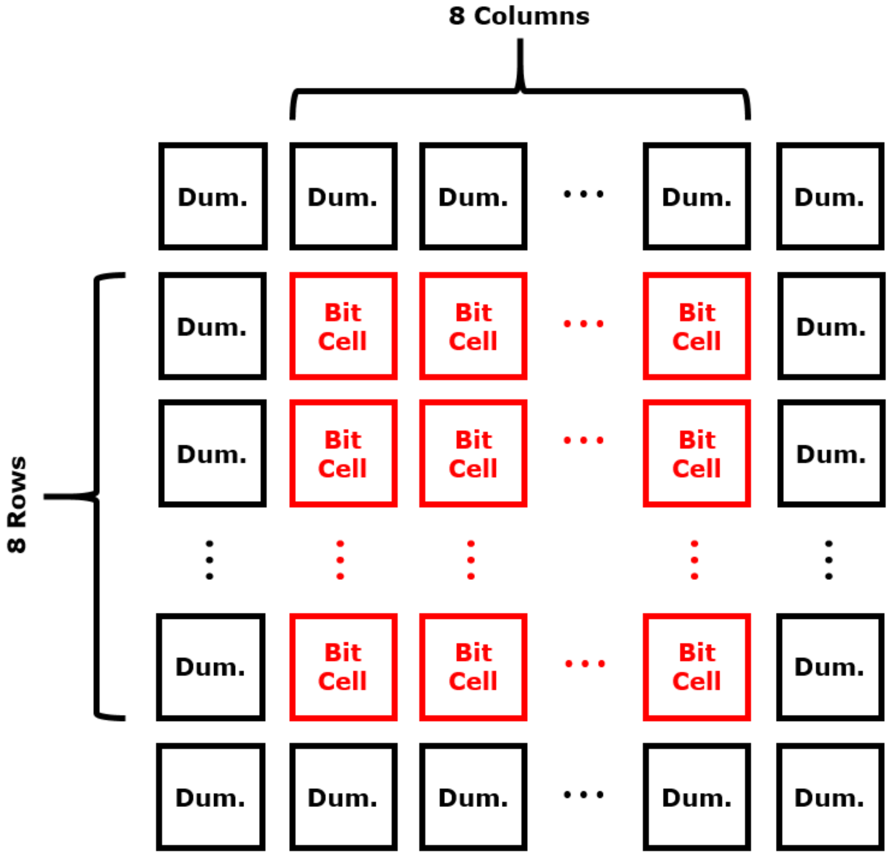


Figure 5.2: Block diagram showing the arrangement of bit cells

64-Bit Array contains 8 × 8 bit cells arranged in a matrix style. Dummies are place around the perimeter to improve the symmetry of the bit array and also block any interference from ambient circuits.

The schematic of this block is shown in Fig. A.3. Each wire of bus **EN<7:0>** are connected to inputs **EN** of all bit cells in each row. Similarly, wires of **TRIG<7:0>** are respectively connected to cells row by row. Complementary outputs of bit cells are respectively connect to bit lines **BIT+<7:0>** and **BIT-<7:0>**.

5.2.2 Trigger

Since there are 64 bit cells in the system, if only use single wire to control the gate of all pre-charge PFETs in bit cells, the fan-out of this wire will be 128, which is unacceptably high. In this case, the block **Trigger** is designed to have 8 outputs, each drives a wire in bus **TRIG**. It is composed of 7 buffers, each of which if formed by two cascaded inverters. As shown in Fig. A.4, the buffers are arranged in a cascaded chain to make a fan-out of 1, 2, 4, 8 for the connections between adjacent stages. In this case, all pre-charge PFETs gates can be fully pulled up to VDD during the ID generation.

5.2.3 Row & Column Counter

The **Row Counter** and the **Column Counter** shares the same topology of a conventional synchronous counter, whose schematic is shown in Fig. A.5. I/Os of this block is listed in Table

Table 5.2: Synchronous counter I/O ports

	Name	Purpose
Inputs	CLK	Clock signal
	CLKINH	Active high. Enabling the clock input.
	CLR	Active low. Resetting the controller.
	EN	Active high. Enabling the counting.
Outputs	Q[2:0]	Present counts
	COUT	Carry out

In the system schematic, **COUT** of the **Column Counter** is connected to **EN** of the **Row Counter** to form a cascaded counter counts from 0 to 63.

Transient simulation results of the counter is shown in Fig. 5.3. When **EN** is active, the counter counts in every clock cycle. Once it counts to 7, the carry out **COUT** is asserted.

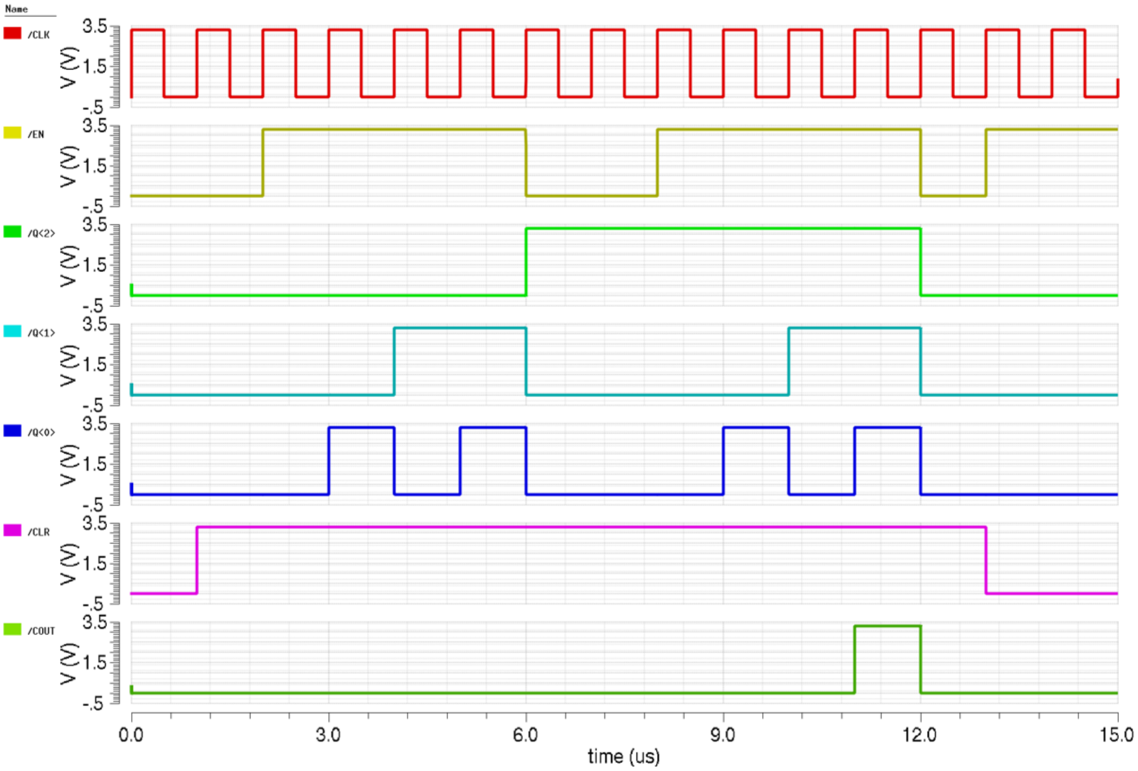


Figure 5.3: Transient simulation result of the synchronous counter

5.2.4 Row & Column Decoder

The structure of both **Row Decoder** and the **Column Decoder** are a 3-to-8 decoder, whose schematic is shown in Fig. A.6 and true table is shown in Table 5.3.

Table 5.3: Truth table of the 3-to-8 decoder

IN<2:0>			OUT<7:0>							
<2>	<1>	<0>	<7>	<6>	<5>	<4>	<3>	<2>	<1>	<0>
0	0	0	0	0	0	0	0	0	0	1
0	0	1	0	0	0	0	0	0	1	0
0	1	0	0	0	0	0	0	1	0	0
0	1	1	0	0	0	0	1	0	0	0
1	0	0	0	0	0	1	0	0	0	0
1	0	1	0	0	1	0	0	0	0	0
1	1	0	0	1	0	0	0	0	0	0
1	1	1	1	0	0	0	0	0	0	0

Inputs IN<2:0> of **Row Decoder** and the **Column Decoder** are respectively connected to the outputs Q<2:0> of **Row Counter** and the **Column Counter**. In this case, when counters are enabled during the readout, bit cells in each row or column can be enabled by the outputs of the two decoders. The transient simulation results of the decoder is shown in Fig 5.4.

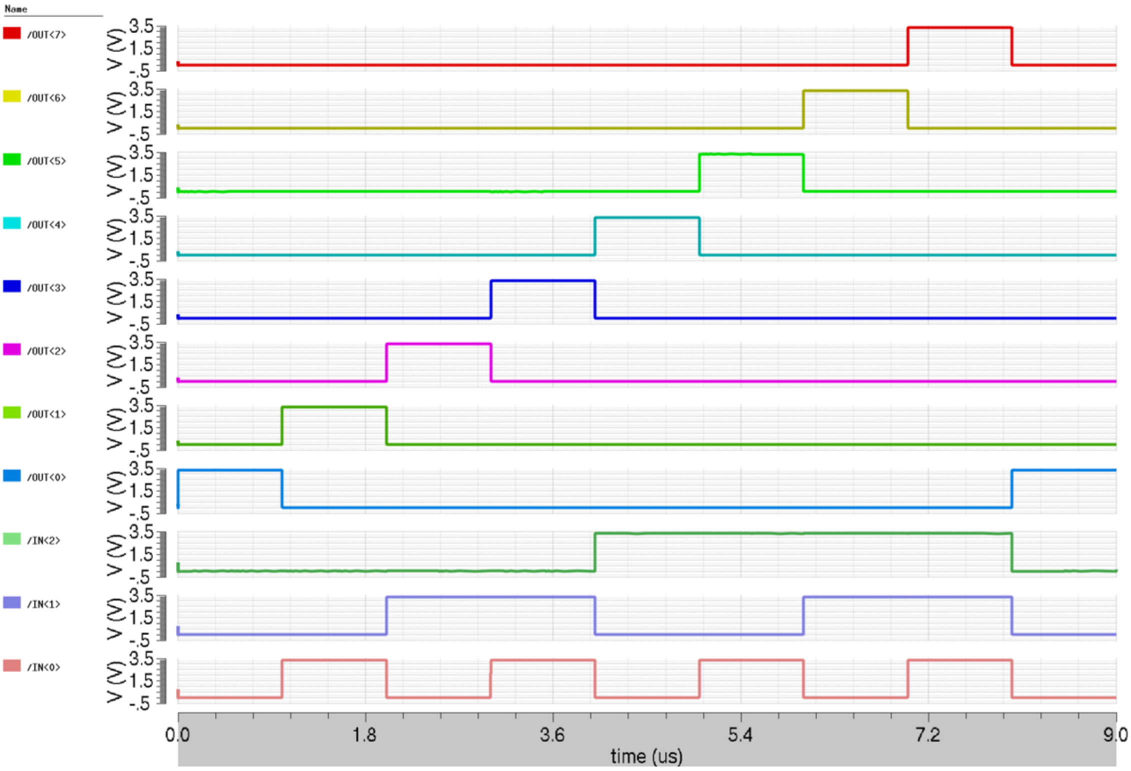


Figure 5.4: Transient simulation result of the 3-to-8 decoder

5.2.5 Sense Amplifier (SA) Array

The **SA Array** is composed of 8 SAs, whose topology is shown in Fig. 5.5.

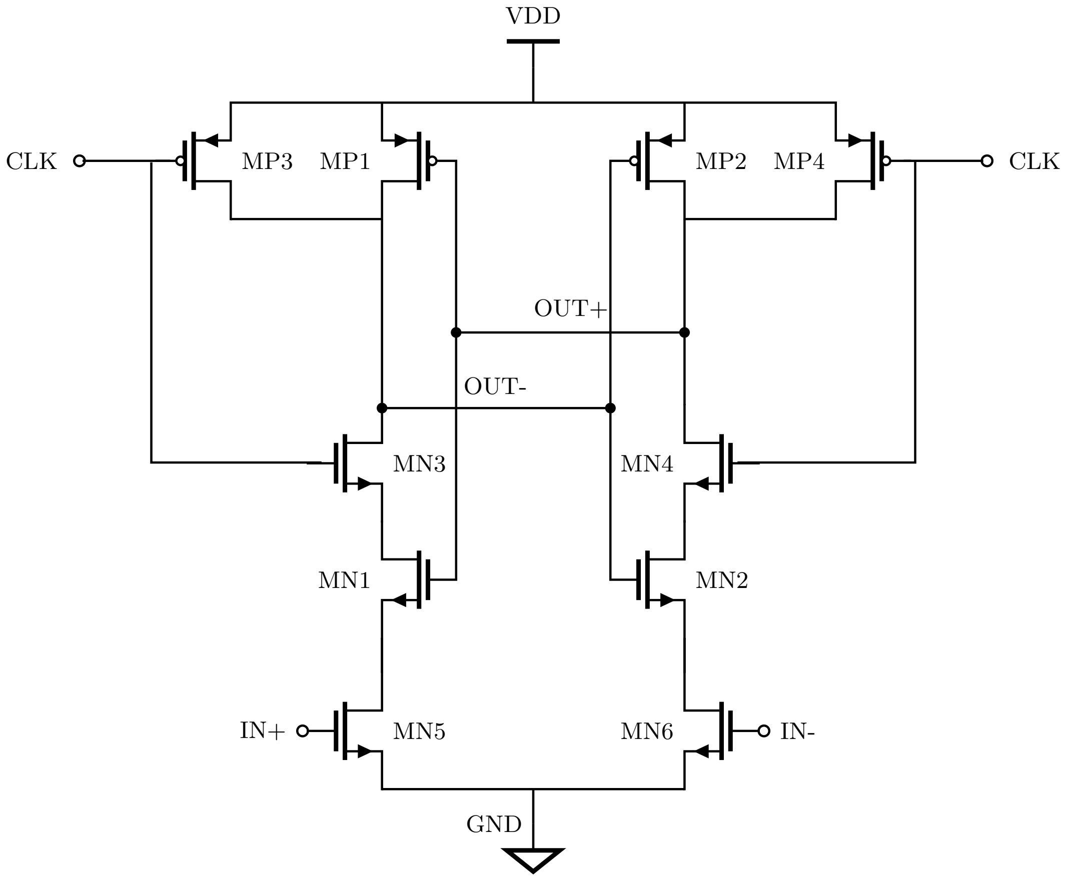


Figure 5.5: Circuit topology of the sense amplifier

Differing from the **Bit Cell** of an **SA-PUF**, in topology of an **SA**, signal **TRIG** is replaced with the clock signal **CLK** and two access NFETs have been removed since outputs of sense amplifiers are evaluated immediately when available. Two NFETs, **MN5** and **MN6**, are sized large to reduce the effect of mismatch to produce an accurate sense of the minor difference of voltages between **IN+** and **IN-**.

The transient simulation result of the **SA**, whose the inputs are connected to the outputs of a **Bit Cell**, is shown in Fig 5.6.

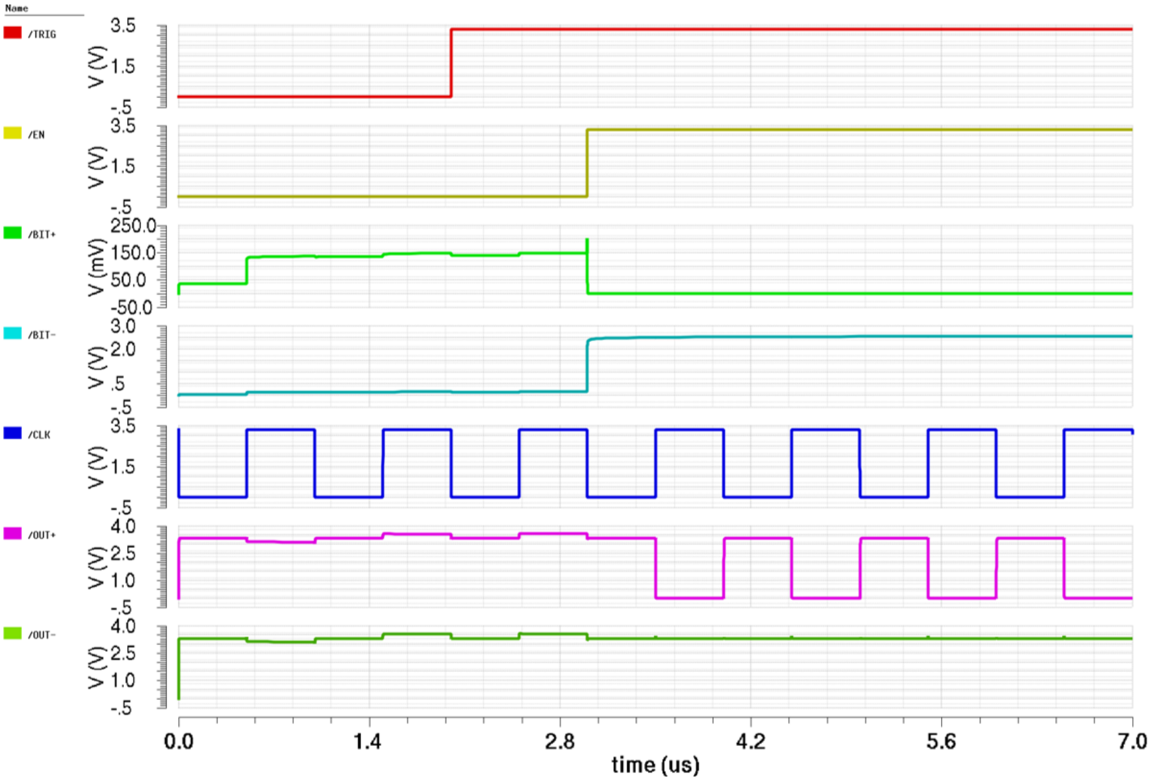


Figure 5.6: Transient simulation result of the sense amplifier with a Bit Cell

During the time when the output of the **Bit Cell** is available after **EN** is activated, the **SA** produce outputs at rising edges of **CLK** for a time with half clock cycle long.

5.2.6 Switch Array

The purpose of the **Switch Array** is to receive the complementary outputs (**OUT+** and **OUT-**) from the **SA Array**, and shunt positive outputs (**OUT+**) to the parallel output ports of the system and negative outputs (**OUT-**) to the serial output ports. It is composed of two independent groups of circuits, an array of 8 **Switch Cells** called the **SOUT Array** and an array of 8 **NAND gates** called the **POUT Array**. The schematic of **Switch Array** is shown in Fig. A.8.

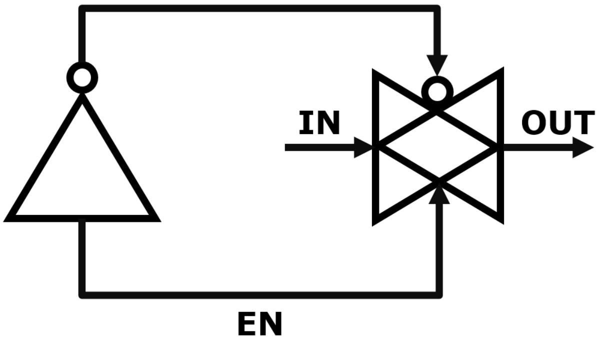


Figure 5.7: Structure of the Switch Cell

Fig. 5.7 shows the structure of a **Switch Cell**, which is composed of a transmission gate and an inverter. The two components are connected in the way shown in the figure so that when the input **EN** is 1, the transmission gate is switched on to allow the transmission of signals.

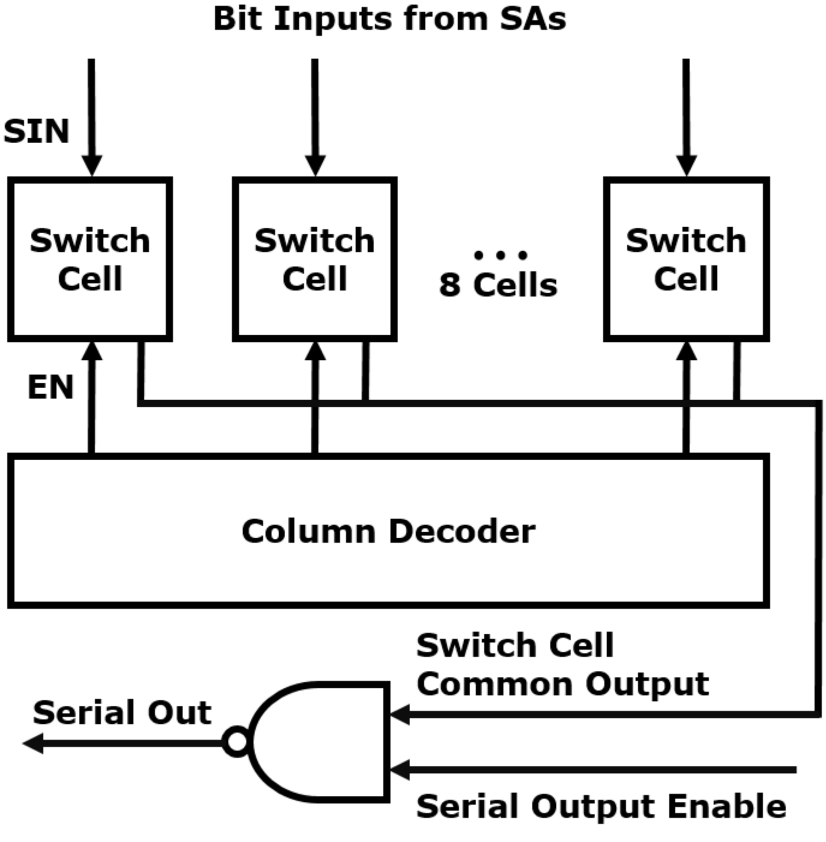


Figure 5.8: Structure of the SOUT Array

As shown in Fig. 5.8, the **SOUT Array** is formed by 8 switch cells, each receiving the output **OUT-** of an **SA**. Outputs of all **Switch Cells** are commonly connected to one input of a NAND gate. The 8 output ports of the **Column Decoder** are connected to 8 switched cells. During the serial readout, after the **SA ARRAY** loads 8 bits in a row, the **Column Decoder** cooperates with the **Column Counter** to enable each **Switch Cell** one by one. When the Serial Output Enable signal, which is connected to the other input of the NAND gate, is activated, the output of the NAND gate produces an inverting bit of the **Switch Cell Common Output**.

Besides the functionality of producing serial outputs, the NAND gate is crucial in the control of power consumption. During idle time of the system when no readout is conducted, outputs of **SAs** are floating. Transmission gates in **Switch Cells** are directly connected to outputs of **SA** without buffering, making the **Switch Cell Common Output** a floating node. the NAND gate can convert the floating voltage to logic 1 by setting **Serial Output Enable** to 0, so that the floating node do not influence the power consumption of the system.

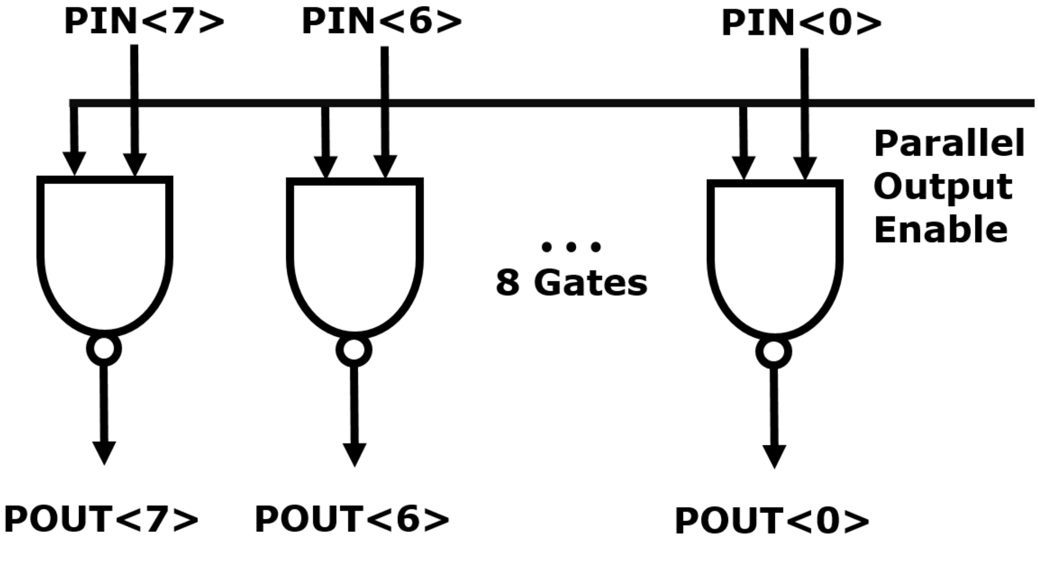


Figure 5.9: Structure of the POUT Array

The structure of the **POUT Array** is simpler than that of the **SOUT Array**. It is composed of 8 NAND gates. one input port of each gate is used to receive outputs of

SAs. The other input of all gates are connect together called **Parallel Output Enable**, which is used to disable all gates and avoid the transmission of floating voltage during idle time.

5.2.7 D-Type Flip-Flop (DFF) with Internal Clock Gating

A low power D-type flip-flop was designed for this system to achieve low dynamic power consumption during the readout. Differing with conventional DFFs, an XOR gate is added to compare the output and the input of the DFF to so that the circuit is clocked only if it receives an input that is different from the original output. The schematic of this circuit is shown in Fig. A.9.

Simulation results of this DFF with consecutive random input digits indicate that the dynamic power has been reduced by 71 times than a DFF without internal clock gating.

5.3 Operation Schemes

5.3.1 ID Generation

Generation Controller Design

I/Os of the **Generation Controller** and their purposes are illustrated Table. 5.4.

Table 5.4: Generation Controller I/O ports

	Name	Purpose
Inputs	CLK	Clock signal
	CLKINH	Active high. Enabling the clock input.
	CLR	Active low. Resetting the controller.
Outputs	RST	Active low. Resetting all system blocks.
	ENG	Active high. Enabling the trigger.
	ENR	Active high. Enabling the Readout Controller.

The **Generation Controller** is design to be executed for only once after being reset in order to complete the ID generation process and then enable the **Readout Controller**. This can be shown by the state transition diagram illustrated in Fig. 5.10 as well as the FSM output table 5.5.

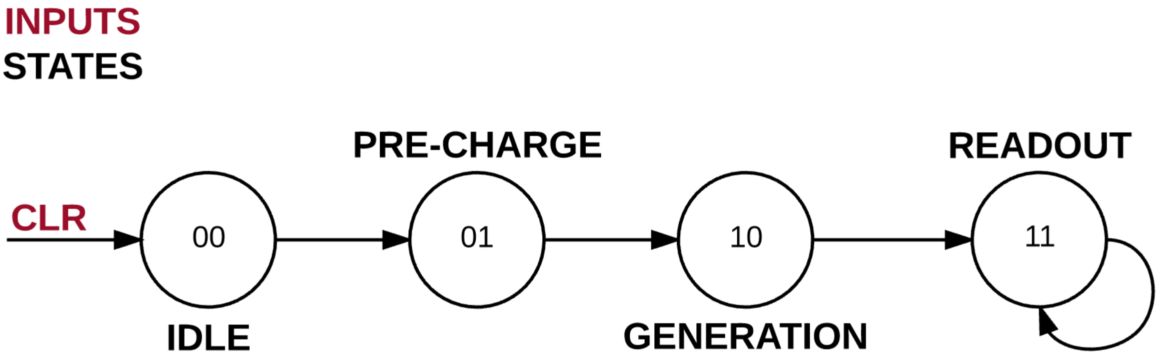


Figure 5.10: State transition diagram of Generation Controller

Table 5.5: Generation Controller outputs v.s. state

State	RST	ENG	ENR
00	0	0	0
01	1	0	0
10	1	1	0
11	1	1	1

Generation Steps

As shown in Fig 5.1, the system input **RESET** is connected to the input **CLR** of the **Generation Controller**. When **RESET** is 0, the **Generation Controller** reset to its initial state, **IDLE**, in which all outputs of the controller are set to 0. Once **RESET** is switched to 1, the **Generation Controller** start to transit to subsequent states in the following consecutive clock cycles. In state **PRE-CHARGE**, output **ENG** is 0 to pre-charge all bit cells. Then in state **GENERATION**, **ENG** becomes 1 to enable the **TRIGGER** to switch **VTRIG** from 0 to 1 so that bit cells generate ID bits. Finally, the FSM runs into state **READOUT** and never transits to another state unless the **RESET** signal is asserted. In this state, **ENR** is switched to 1 to enables the **Readout Controller**.

5.3.2 ID Readout

Readout Controller Design

I/Os of the **Readout Controller** and their purposes are illustrated Table. 5.6.

Table 5.6: Readout Controller I/O ports

	Name	**Purpose**
Inputs	CLK	Clock signal
	CLKINH	Active high. Enabling the clock input.
	CLR	Active low. Resetting the controller.
	MODE	0 for Serial Output and 1 for 8-Bit Output.
	START	Active high. Starting the readout.
	END	Active high. Feedback indicating the end of readout.
Outputs	P	Active high. Enabling readout for 8-bit outputs.
	S	Active high. Enabling readout for serial outputs.

This controller is responsible for determining if the requester requires a serial ID or an ID in 8-bit sections and enabling the readout process. For this purpose, the controller has two outputs **P** and **S**, which are respectively for enabling the serial readout and 8-bit parallel readout.

The state transition diagram and outputs table of this controller is respectively shown in Fig. 5.11 and Table 5.7.

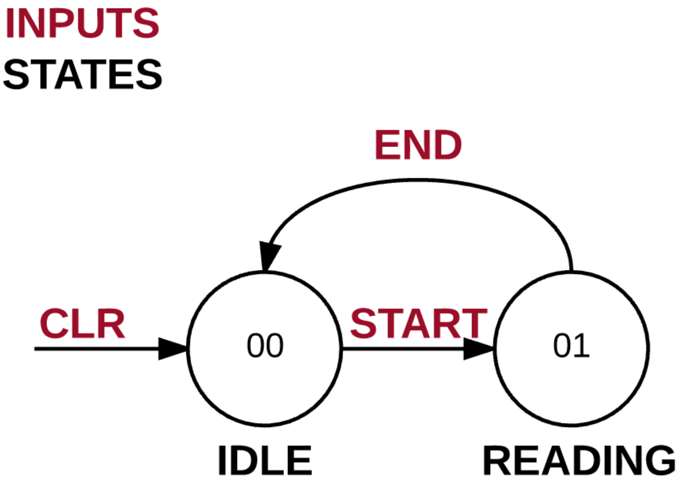


Figure 5.11: State transition diagram of Readout Controller

Table 5.7: Readout Controller outputs v.s. state and inputs

State	MODE	S	P
0	0	0	0
0	1	0	0
1	0	1	0
1	1	0	1

According to the value of **MODE**, once **START** is asserted, the controller runs into state **READING**. Differing from the **Generation Controller**, **Readout Controller** is a Mealy machine, which means that its output values are determined by both the present state and the inputs. As shown in Table 5.7, in state **READING**, output **S** is activated when **MODE** is 0 and **P** is activated when **MODE** is 1. To determine when the readout process is finished, a feedback signal indicating the end of the readout is forwarded to the input **END** to make the FSM return the **IDLE** state.

Readout Process

In serial readout mode, once **START** is set to 1, the **Readout Controller** enables both the row counter and the column counter. The carry out **COUT** of the column counter is forwarded to the enable port **EN** of the row counter. In this case, outputs of all bit cells can be iterated over and read one by one. In parallel readout mode, only the row counter is enabled so that bits in the array are read row by row.

5.4 Strategies for Reducing Power

Despite the low power DFF, some system level design has been used to reduce the total power consumption. For example, as shown in the schematic of the system (Fig. A.1), the **64-Bit Array** is power gated by using a PFET, of which the gate is connected to the inverted **RST** signal produced by the **Generation Controller**. In this case, the **64-Bit Array** can only be powered on when necessary.

Moreover, all clocked blocks contains an input called **CLKINH**, which is used to conduct the clock gating. For example, the clock signal of **Generation Controller** is blocked after the completion of generation to reduce dynamic power. Furthermore, a more complex combinational logic block was designed to control the clock signal connected to the **Sense Amplifier Array** so that **SAs** are only clocked when output on bit lines are valid.

5.5 System Layout

Fig.5.12 shows the layout of the system excluding the pad ring.

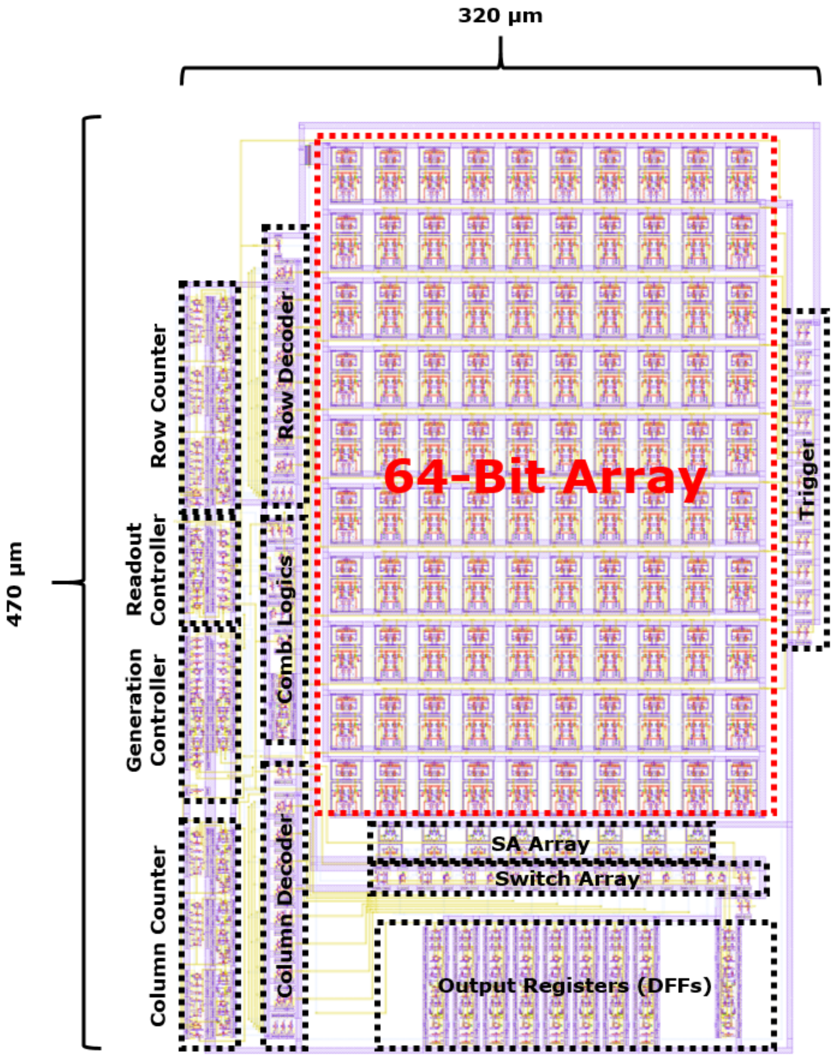


Figure 5.12: Layout of the whole system

Totally 3 layers of metal (M1-M3) are used. M1 and M2 are used for connection within standard cells. M2 and M3 are used for most interconnections between cells or blocks. The dimension of the layout is 470 μm × 320 μm, which gives an approximate area of 0.15 mm^2.

5.6 Simulation Results & Discussion

5.6.1 8-Bit Parallel Readout Timing

Transient simulation results of the system in parallel readout mode is shown in Fig. 5.13.

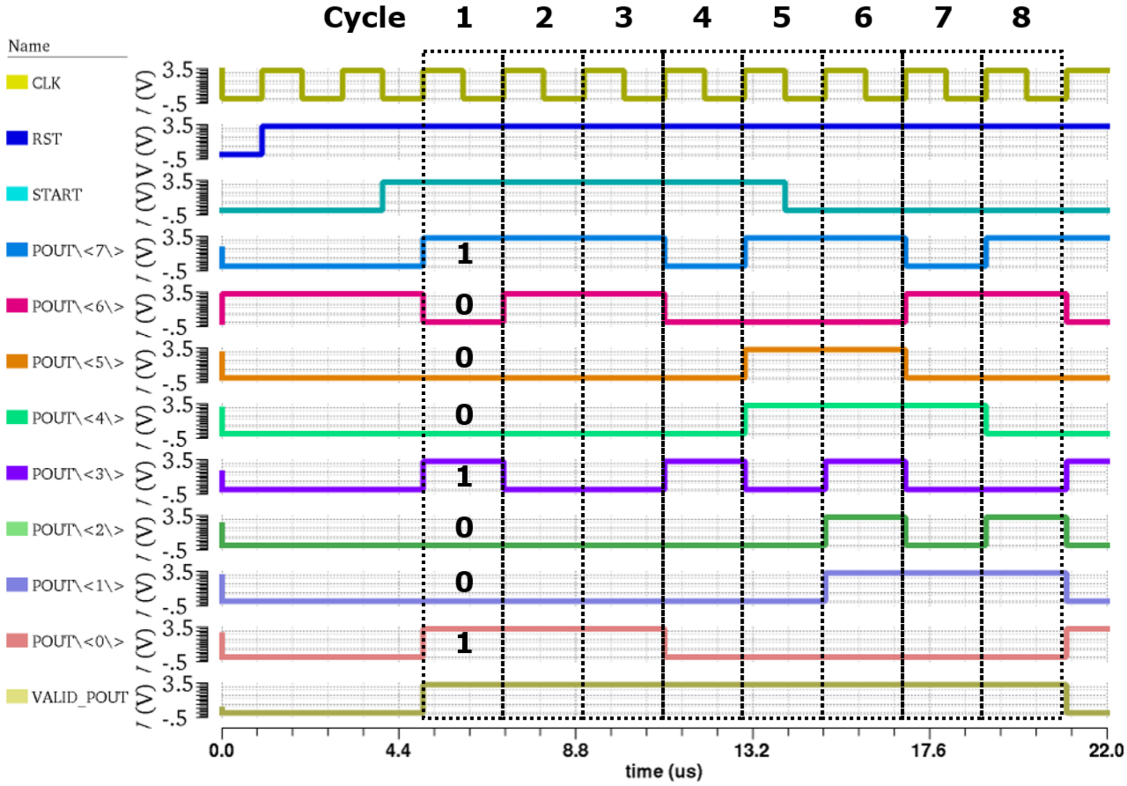


Figure 5.13: Transient simulation result of the system during parallel readout (MODE=1)

START signal is activated after the system is reset, then **VALID_POUT** is asserted to indicate the validity of ID outputs. As shown in the figure, the 8-bit ID section is 10001001, and it takes another 7 cycles to produce all rest sections.

6 pJ/bit generation 2.6 pJ for consecutive readout

5.6.2 Serial Readout Timing

Fig. 5.14 shows the transient simulation results of the system in serial readout mode. Similarly, bits are available after the activation of signal **START** when signal **VALID_SOUT** is asserted and it takes 64 clock cycles to produce all ID bits.

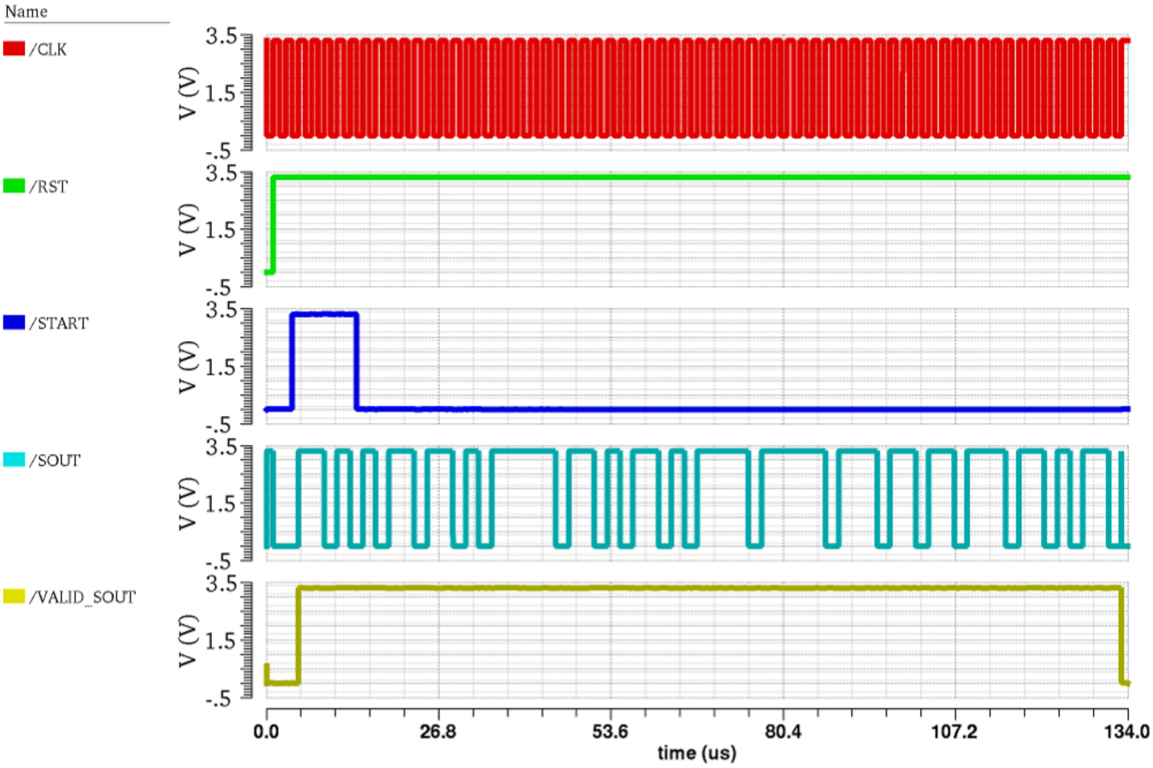
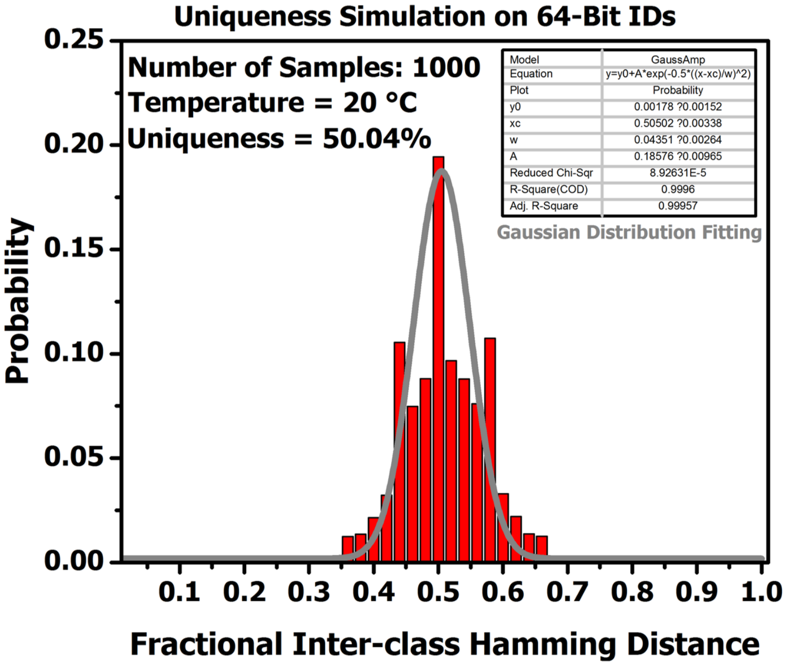


Figure 5.14: Transient simulation result of the system during serial readout (MODE=1)

5.6.3 Uniqueness of Generated IDs

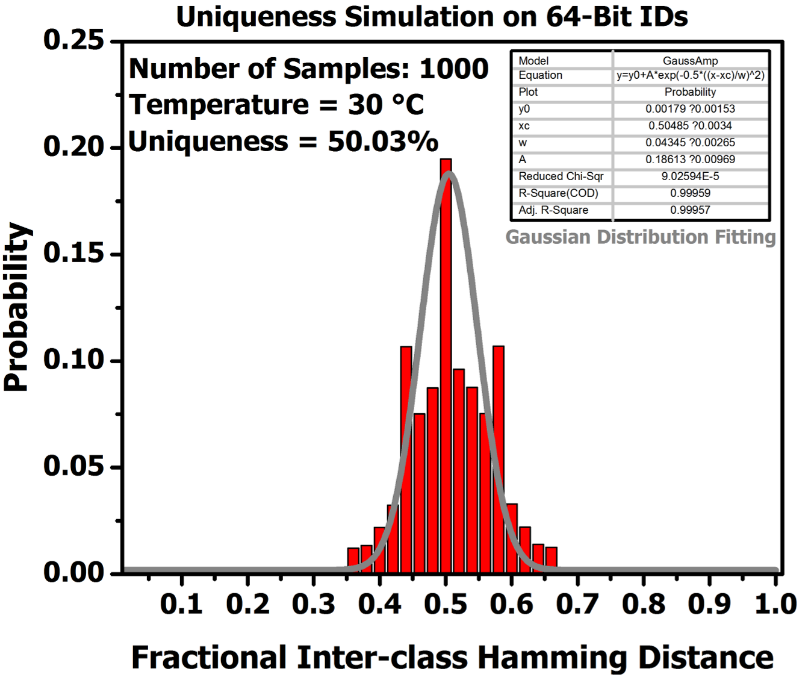
By conducting Monte Carlo simulation on 1000 **Bit Array** samples at 3 temperature points (20°C, 30°C, 40°C) closed to the range of human body temperature, the probability distributions of fractional inter-class HD of generated IDs is shown in Fig. 5.15, 5.16, and 5.17.

It can be seen from the Gaussian distribution fittings parameters that the distribution of fractional inter-class HD merely changes with the variation of temperature. The uniqueness of generated IDs under the 3 temperature points are respectively, 50.04%, 50.03% and 50.03%, which are all close to the ideal value 50%.



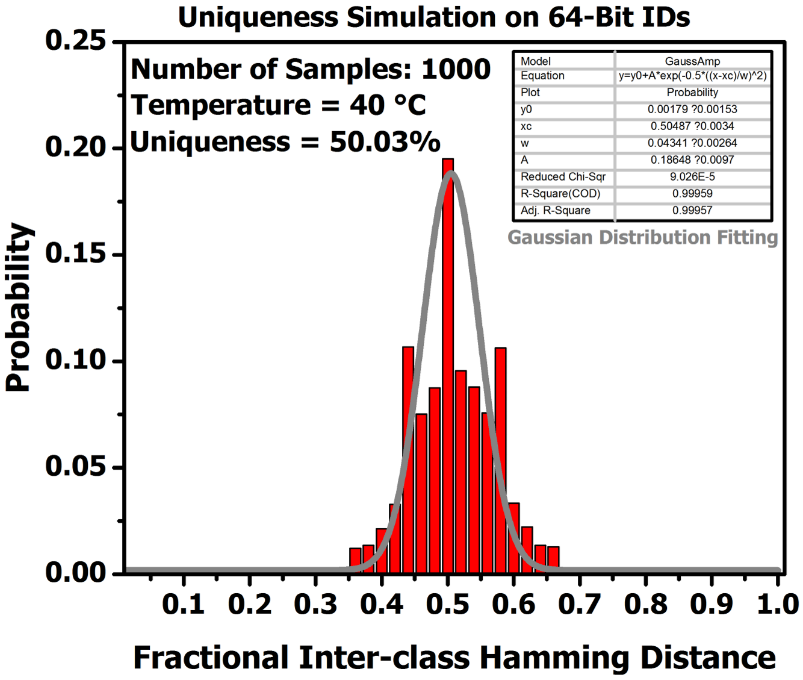
Model	GaussAmp
Equation	y=y0+A*exp(-0.5*((x-xc)/w)^2)
Plot	Probability
y0	0.00178 ?0.00152
xc	0.50502 ?0.00338
w	0.04351 ?0.00264
A	0.18576 ?0.00965
Reduced Chi-Sqr	8.92631E-5
R-Square(COD)	0.9996
Adj. R-Square	0.99957

Figure 5.15: Probability distribution of fractional inter-class hamming distance of generated IDs at 20°C



Model	GaussAmp
Equation	y=y0+A*exp(-0.5*((x-xc)/w)^2)
Plot	Probability
y0	0.00179 ?0.00153
xc	0.50485 ?0.0034
w	0.04345 ?0.00265
A	0.18613 ?0.00969
Reduced Chi-Sqr	9.02594E-5
R-Square(COD)	0.99959
Adj. R-Square	0.99957

Figure 5.16: Probability distribution of fractional inter-class hamming distance of generated IDs at 30°C



Model	GaussAmp
Equation	y=y0+A*exp(-0.5*((x-xc)/w)^2)
Plot	Probability
y0	0.00179 ?0.00153
xc	0.50487 ?0.0034
w	0.04341 ?0.00264
A	0.18648 ?0.0097
Reduced Chi-Sqr	9.026E-5
R-Square(COD)	0.99959
Adj. R-Square	0.99957

Figure 5.17: Probability distribution of fractional inter-class hamming distance of generated IDs at 40°C

5.6.4 Power Consumption

The power consumption of the system is obtained from post layout simulation, and is shown in Table 5.8.

Table 5.8: Power consumption of the system (Clock Frequency = 1 MHz)

Mode	Energy/Bit	Average Power (Generation+Readout)
Parallel	6.0 pJ	21.0 μW
Serial	17.3 pJ	8.0 μW

The results were measured from the power-up of the system to the moment when all bits are read out. The energy consumption in serial readout mode is distinctly higher that in the parallel readout mode, which is due to the usage of **Column Decoder** and **Column Counter** in the serial readout mode. However, the average power in the parallel readout mode is larger than that in the serial readout mode. This is because most of energy is consumed during the bit generation process, which happens before the readout. Furthermore, it takes far more cycles to read all bits in the serial readout mode than in the parallel mode. In this case, the actual average power of the system should be lower than the simulated value in practical applications, since in most time the system is idle.

5.7 Comparison with Other Works

Table 5.9: Comparison of performance between this work and other works

	PUF Type	**Uniqueness**	**Energy/Bit**	**Technology**
This work	SA	50.04%	6.0 pJ	350 nm
Bhargava et al. [27]	SA	50.00%	Not Available	65 nm
Lim et al. [13]	Arbiter	1.05%	Not Available	Not Available
Suh et al. [1]	RO	46.15%	Not Available	180 nm
Cortez et al. [28]	SRAM	48%±2.3%	Not Available	45 nm
Su et al. [29]	SRAM-like	50.13%	1.6 pJ	180 nm
Chen et al. [30]	BR	50.90%	Not Available	Not Available
Lofstrom et al. [31]	Customized	Not Available	8330 pJ	350 nm
Tang et al. [3]	Antenna Effect	50.47%	1.2 pJ	180 nm
Liu et al. [23]	Oxide Breakdown	49.94%	Not Available	65 nm

As shown in Table 5.9, the proposed PUF system achieved the second highest uniqueness among all listed works. The energy consumption per bit for the parallel readout mode was used to be compared with other works, though the energy consumption data are not available for most other works. The work proposed by Tang et al. [3] achieved the lowest energy consumption per bit, but it was implemented on the 180 nm technology, which is more advanced than that used for this work.

However, all results of this work in the table was obtained by simulations. The actual performance of the system after tape-out is unknown, while results of most other works are based on measurements of fabricated chips. In this case, the final on-chip performance of this system may have difference with the presented results and should be further evaluated after tape-out in the future.

Chapter 6

Conclusion

6.1 Conclusion

IN multi-node implantable devices, CMOS-compatible on-chip unique identification generation is necessary for the master device to establish correct communications with slave chips. The PUF, which is a promising solution for on-chip ID generation and has applications in many microelectronic industries, has been paid extensive concentration recently. For many years, numerous scientists have proposed various PUF designs which are suitable for utilizations in diverse scenarios and for being implemented on different chips, such as FPGAs and ASICs.

Inspired by the operation principle of conventional sense amplifiers, this project aims at designing an on-chip ID generation system for multi-node implantable devices. Apart for the realization of ID generation functionality, considerations on design of the module includes power consumption due to limited capacity of battery.

In this thesis, a novel SA-PUF **Bit Cell** structure has been presented. The proposed **Bit Cell** design has achieved the uniformity close to 50% and good robustness with respect to the variation of human body temperature. Moreover, a design of an power-efficient ID generation system has been completed to be able to produce high quality IDs and provide readout functionality. According to evaluations through Monte Carlo simulations, IDs generated by the system has been found to have high uniqueness compared to other works based on diverse PUF structures. Furthermore, in order to reduce the overall power consumption, considerations have been paid on circuit level optimizations of the DFF as well as system level clock & power gating strategies.

6.2 Limitations & Future Works

At the current stage, the chips of this ID generation system have not been fabricated, and thus all results obtained are based on simulations. In this case, the performance of the system in practical applications may differ from that assessed in Monte Carlo simulations. Due to this problem, the reliability of this PUF structure has not been evaluated, which should be determined by measuring the average fractional intra-class hamming distance (Eq. 2.2) of IDs produced by a fabricated sample. Since the layout has been finished, in the future, the chip should be fabricated so that quality metrics of the PUF can be measured in real life. To do so, the performance of the proposed system can be more precisely determined. Moreover, some of the output bits can be unstable to be flipped during runtime of the ID generation system. Al though ideally 64-bit ID can identify 2^{64} chips, the practical number can not be as large as that. Methods such as fuzzy extractor can be developed in the future to further improve the identifiability of the system.

The read stability of **Bit Cells** is another significant property of the system that has not been assessed. During the readout process, when rows in the **64-Bit Array** are enabled one by one, residual charges on bit lines with large parasitic capacitance might affect the internal state of **Bit Cells** when enabled. In the future, the robustness of **Bit Cells** with respect to the influence of voltage on the bit line should be studied and characterised by simulations and measurement. Finally, the robustness of the **Bit Cell** against supply variations is not as good as that with respect to the temperature. This should be further studied to improve the robustness of the system.

Bibliography

[1] G. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” 2007, pp. 9–14.

[2] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rhrmair, “The bistable ring puf: A new architecture for strong physical unclonable functions,” in *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, June 2011, pp. 134–141.

[3] F. Tang, D. G. Chen, B. Wang, A. Bermak, A. Amira, and S. Mohamad, “Cmos on-chip stable true-random id generation using antenna effect,” *IEEE Electron Device Letters*, vol. 35, no. 1, pp. 54–56, Jan 2014.

[4] D. W. Bauder, “An Anti - Counterfeiting Concept for Currency Systems,” 1983.

[5] P. S. Ravikanth, “Physical one-way functions,” Ph.D. dissertation, Massachusetts Institute of Technology, 2001.

[6] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, “Silicon physical random functions,” in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ser. CCS ’02. New York, NY, USA: ACM, 2002, pp. 148–160. [Online]. Available: http://doi.acm.org/10.1145/586110.586132

[7] M. J. M. Pelgrom and A. C. J. Duinmaijer, “Matching properties of mos transistors,” in *Solid-State Circuits Conference, 1988. ESSCIRC ’88. Fourteenth European*, Sept 1988, pp. 327–330.

[8] P. G. Drennan and C. C. McAndrew, “Understanding mosfet mismatch for analog design,” *IEEE Journal of Solid-State Circuits*, vol. 38, no. 3, pp. 450–456, Mar 2003.

[9] X. Tang, V. K. De, and J. D. Meindl, “Intrinsic mosfet parameter fluctuations due to random dopant placement,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 5, no. 4, pp. 369–376, Dec 1997.

[10] A. J. Bhavnagarwala, X. Tang, and J. D. Meindl, “The impact of intrinsic device fluctuations on cmos sram cell stability,” *IEEE Journal of Solid-State Circuits*, vol. 36, no. 4, pp. 658–665, Apr 2001.

[11] M. Kalyanaraman and M. Orshansky, “Novel strong puf based on nonlinearity of mosfet subthreshold operation,” in *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on*, June 2013, pp. 13–18.

[12] J. Guajardo, S. S. Kumar, K. Kursawe, G.-J. Schrijen, and P. Tuyls, *Intrinsic Physical Unclonable Functions in Field Programmable Gate Arrays.* Wiesbaden: Vieweg, 2007, pp. 313–321. [Online]. Available: http://dx.doi.org/10.1007/978-3-8348-9418-2_33

[13] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, “Extracting secret keys from integrated circuits,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200–1205, Oct 2005.

[14] A. Maiti and P. Schaumont, “Improving the quality of a physical unclonable function using configurable ring oscillators,” in *2009 International Conference on Field Programmable Logic and Applications*, Aug 2009, pp. 703–707.

[15] C. E. Yin, G. Qu, and Q. Zhou, “Design and implementation of a group-based ro puf,” in *Design, Automation Test in Europe Conference Exhibition (DATE), 2013*, March 2013, pp. 416–421.

[16] R. Maes and I. Verbauwhede, *Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 3–37. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-14452-3_1

[17] M. K. Mandal and B. C. Sarkar, "Ring oscillators: Characteristics and applications," *Indian Journal of Pure & Applied Physics*, vol. 48, pp. 136–145, 2010. [Online]. Available: http://nopr.niscair.res.in/bitstream/123456789/7244/1/IJPAP%2048(2)%20136-145.pdf

[18] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, *FPGA Intrinsic PUFs and Their Use for IP Protection.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 63–80. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-74735-2_5

[19] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up sram state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, Sept 2009.

[20] S. Fang and J. P. McVittie, "Thin-oxide damage from gate charging during plasma processing," *IEEE Electron Device Letters*, vol. 13, no. 5, pp. 288–290, May 1992.

[21] H. Shin, K. Noguchi, and C. Hu, "Modeling oxide thickness dependence of charging damage by plasma processing," *IEEE Electron Device Letters*, vol. 14, no. 11, pp. 509–511, Nov 1993.

[22] W. Maly, C. Ouyang, S. Ghosh, and S. Maturi, "Detection of an antenna effect in vlsi designs," in *Defect and Fault Tolerance in VLSI Systems, 1996. Proceedings., 1996 IEEE International Symposium on*, Nov 1996, pp. 86–94.

[23] N. Liu, S. Hanson, D. Sylvester, and D. Blaauw, "Oxid: On-chip one-time random id generation using oxide breakdown," in *2010 Symposium on VLSI Circuits*, June 2010, pp. 231–232.

[24] Y. C. Huang, T. Y. Yew, W. Wang, Y. H. Lee, R. Ranjan, N. K. Jha, P. J. Liao, J. R. Shih, and K. Wu, "Re-investigation of gate oxide breakdown on logic circuit reliability," in *Reliability Physics Symposium (IRPS), 2011 IEEE International*, April 2011, pp. 2A.4.1–2A.4.6.

[25] J. A. Marx, R. S. Hockberger, R. M. Walls, M. H. Biros, D. F. Danzl, M. Gausche-Hill, A. Jagoda, FACEP, L. J. Ling, E. J. Newton, B. J. Zink, and A. P. of English John Marx, *Rosen's emergency medicine - concepts and clinical practice*, 8th ed. London: Elsevier, 05 2006.

[26] G. C. Cook, A. I. Zumla, J. Farrar, P. J. Hotez, and T. Junghanss, *Manson's Tropical Diseases: Expert Consult.* Saunders, 2008.

[27] M. Bhargava, C. Cakir, and K. Mai, "Attack resistant sense amplifier based pufs (sa-puf) with deterministic and controllable reliability of puf responses," in *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*, June 2010, pp. 106–111.

[28] M. Cortez, S. Hamdioui, and R. Ishihara, "Design dependent sram puf robustness analysis," in *2015 16th Latin-American Test Symposium (LATS)*, March 2015, pp. 1–6.

[29] Y. Su, J. Holleman, and B. P. Otis, "A digital 1.6 pj/bit chip identification circuit using process variations," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 1, pp. 69–77, Jan 2008.

[30] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rhrmair, "Characterization of the bistable ring puf," in *2012 Design, Automation Test in Europe Conference Exhibition (DATE)*, March 2012, pp. 1459–1462.

[31] K. Lofstrom, W. R. Daasch, and D. Taylor, "Ic identification circuit using device mismatch," in *Solid-State Circuits Conference, 2000. Digest of Technical Papers. ISSCC. 2000 IEEE International*, Feb 2000, pp. 372–373.

Appendix A

Schematics

A.1 System

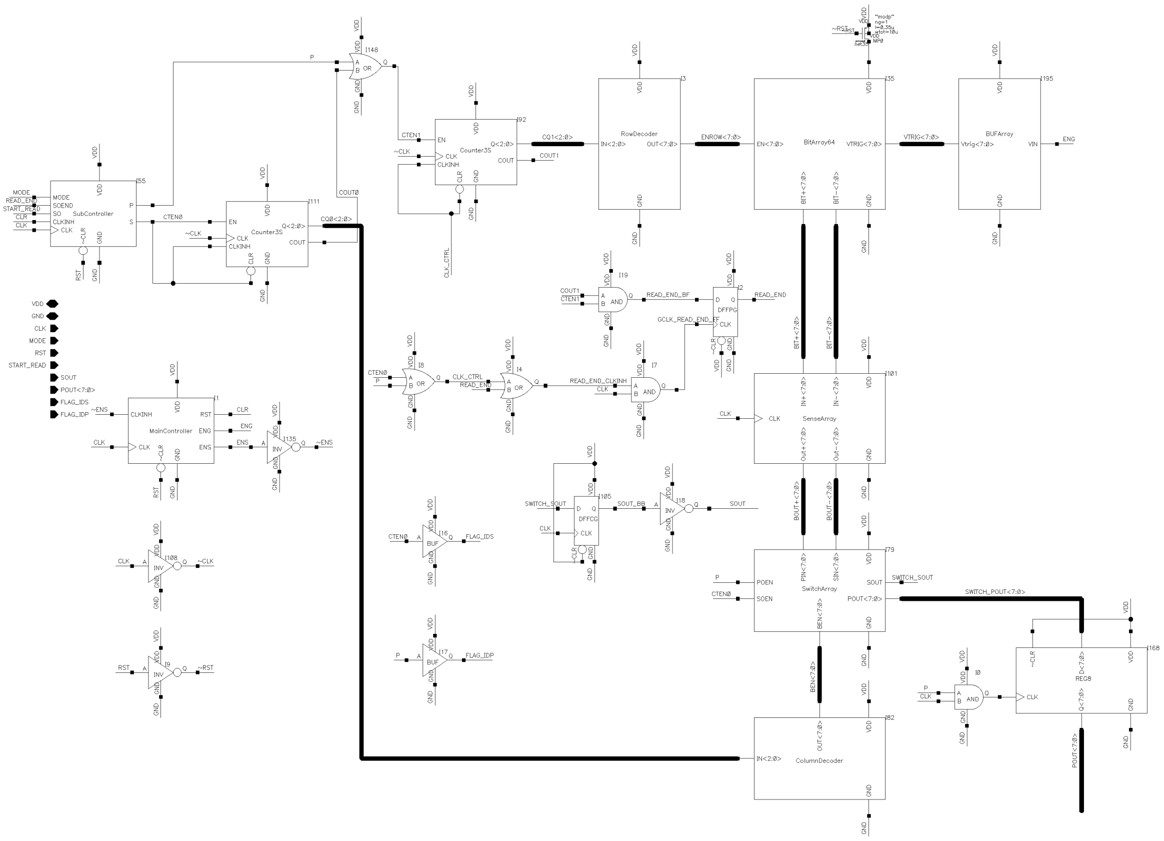


Figure A.1: Schematic of the system

A.2 Bit Cell

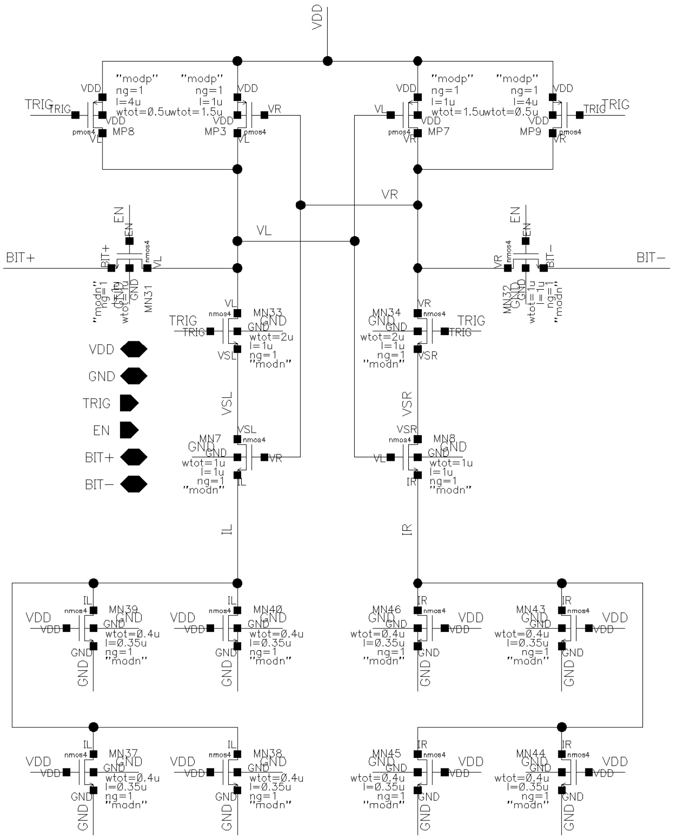


Figure A.2: Schematic of Bit Cell

A.3 64-Bit Array

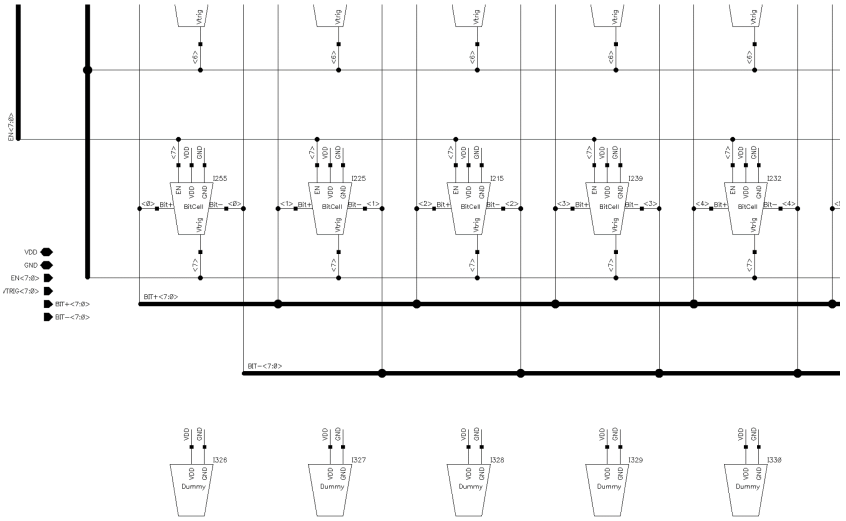


Figure A.3: Partial schematic of 64-Bit Array

A.4 Trigger

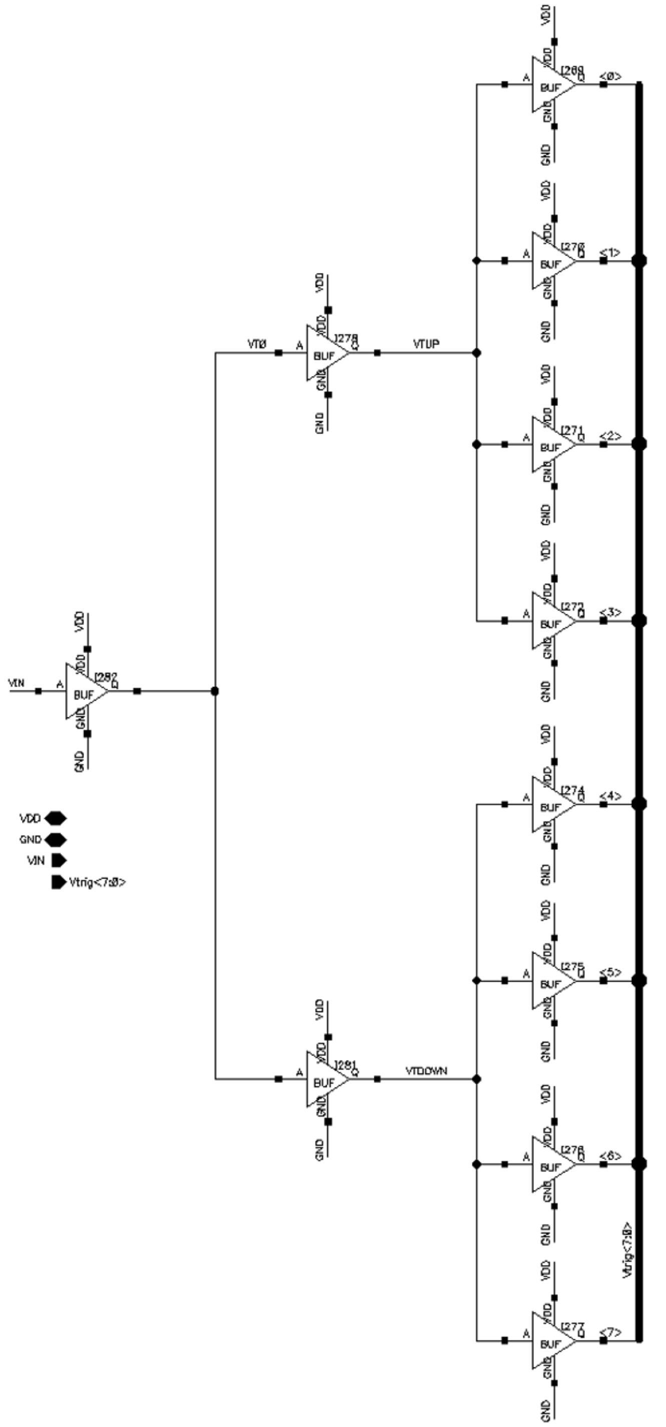


Figure A.4: Schematic of Trigger

A.5 Synchronous Counter

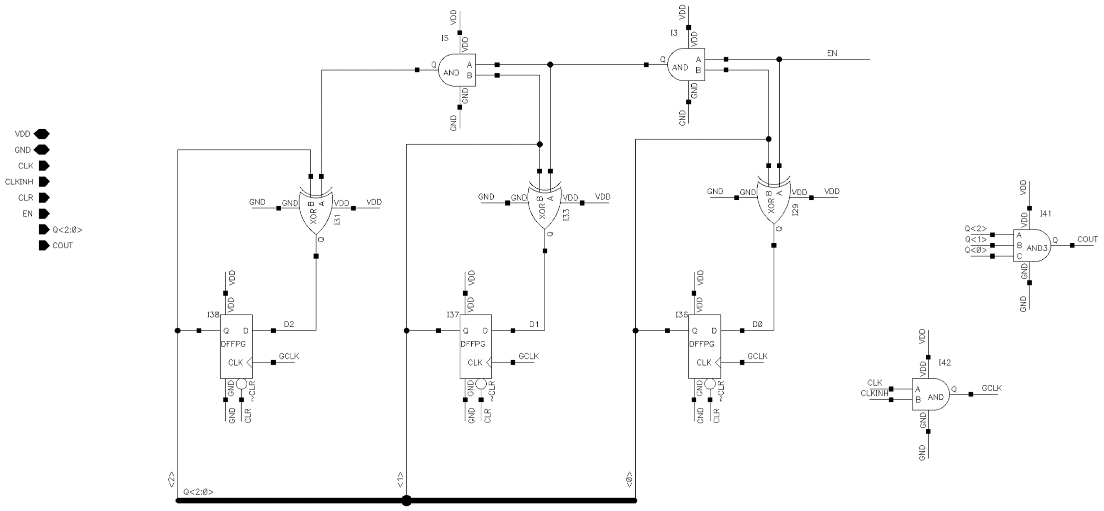


Figure A.5: Schematic of the synchronous counter

A.6 3-to-8 Decoder

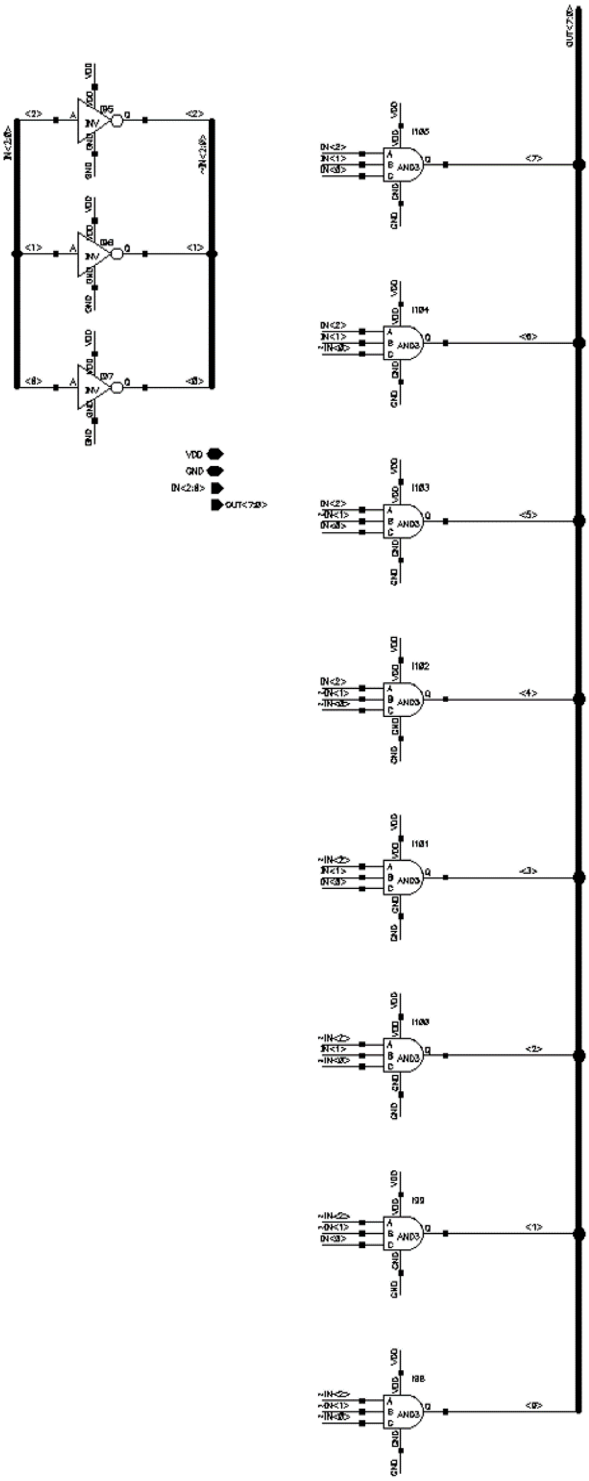


Figure A.6: Schematic of the 3-to-8 decoder

A.7 Sense Amplifier

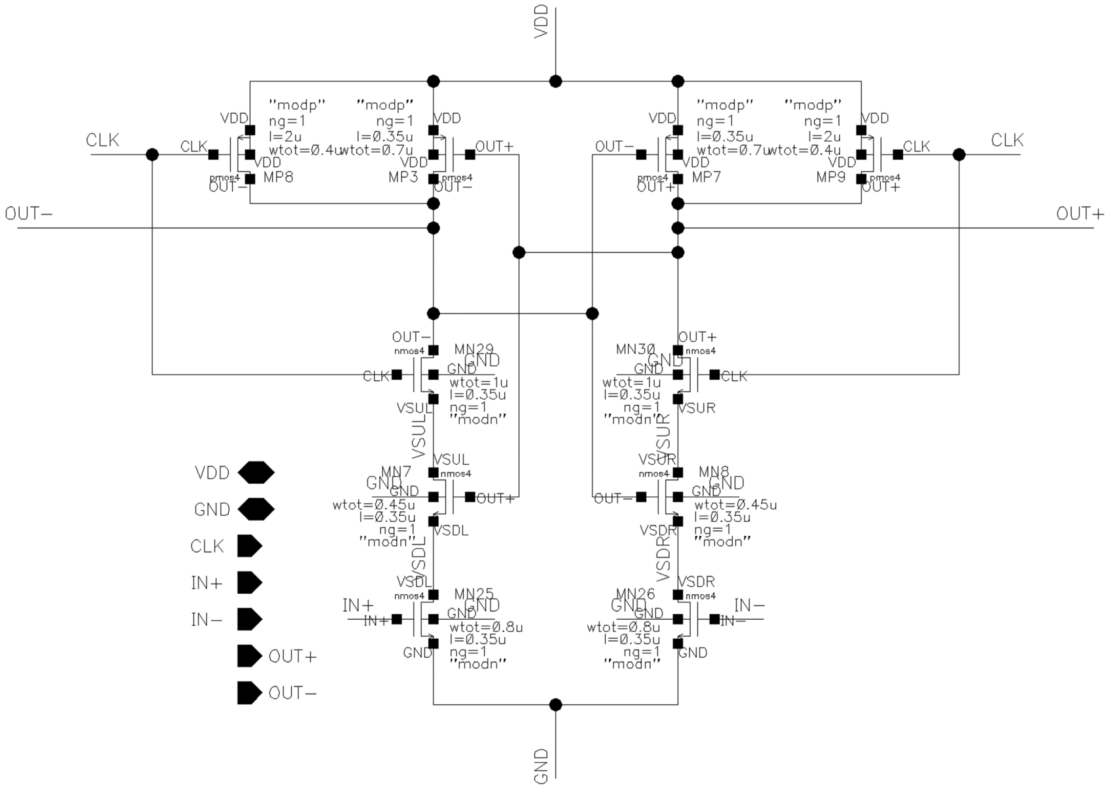


Figure A.7: Schematic of the sense amplifier

A.8 Switch Array

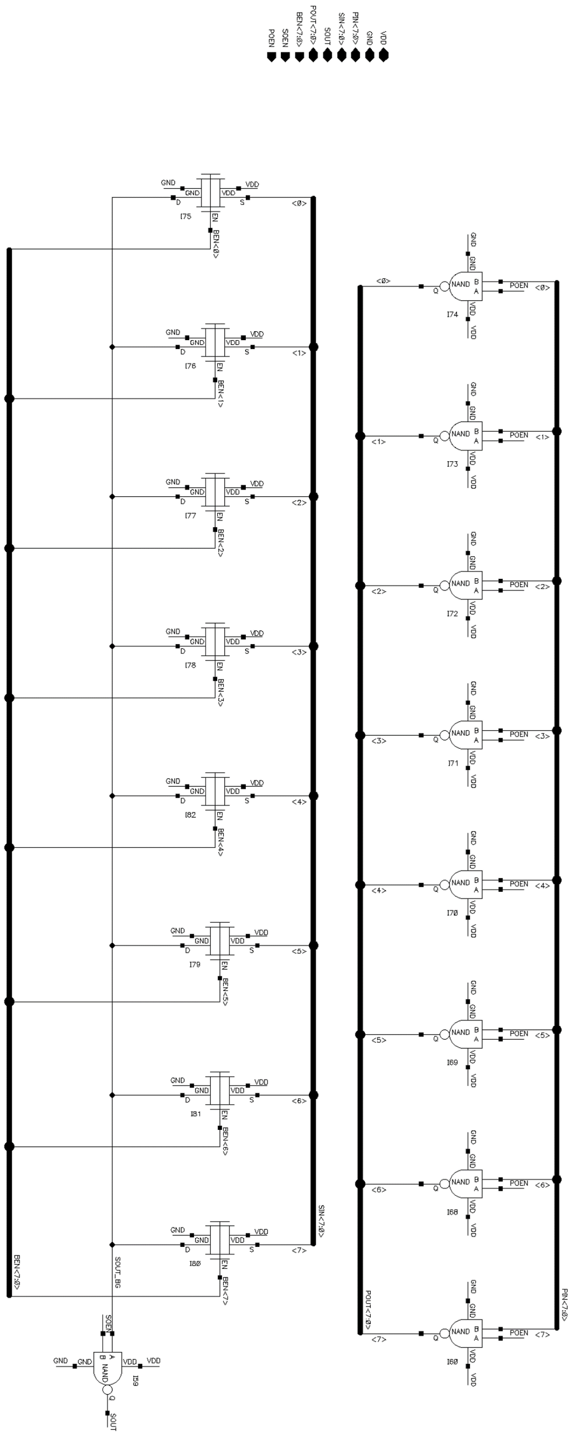


Figure A.8: Schematic of the switch array

A.9 D-Type Flip-Flop with Internal Clock & Power Gating

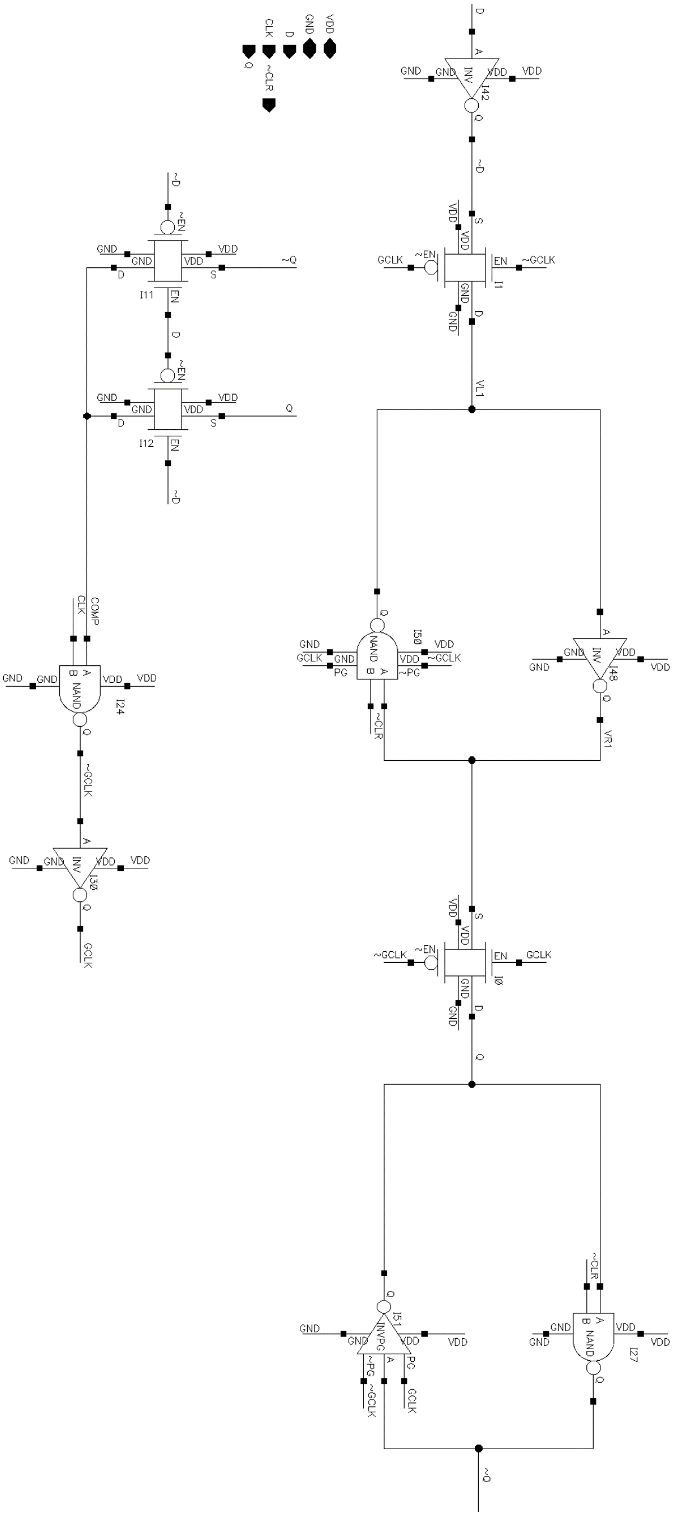


Figure A.9: Schematic of the D-type flip-flop with internal clock & power gating

A.10 Generation Controller

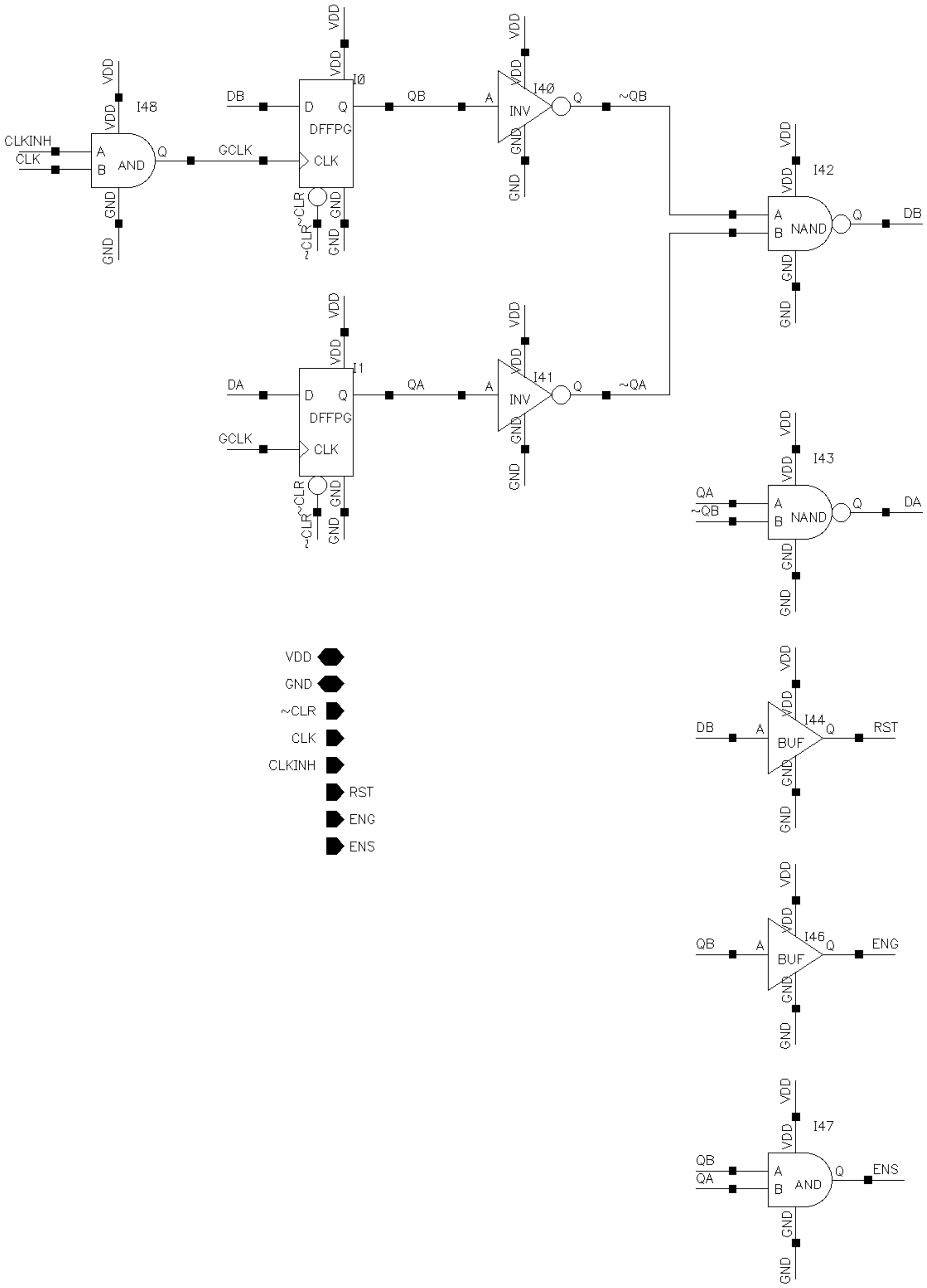


Figure A.10: Schematic of the Generation Controller

A.11 Readout Controller

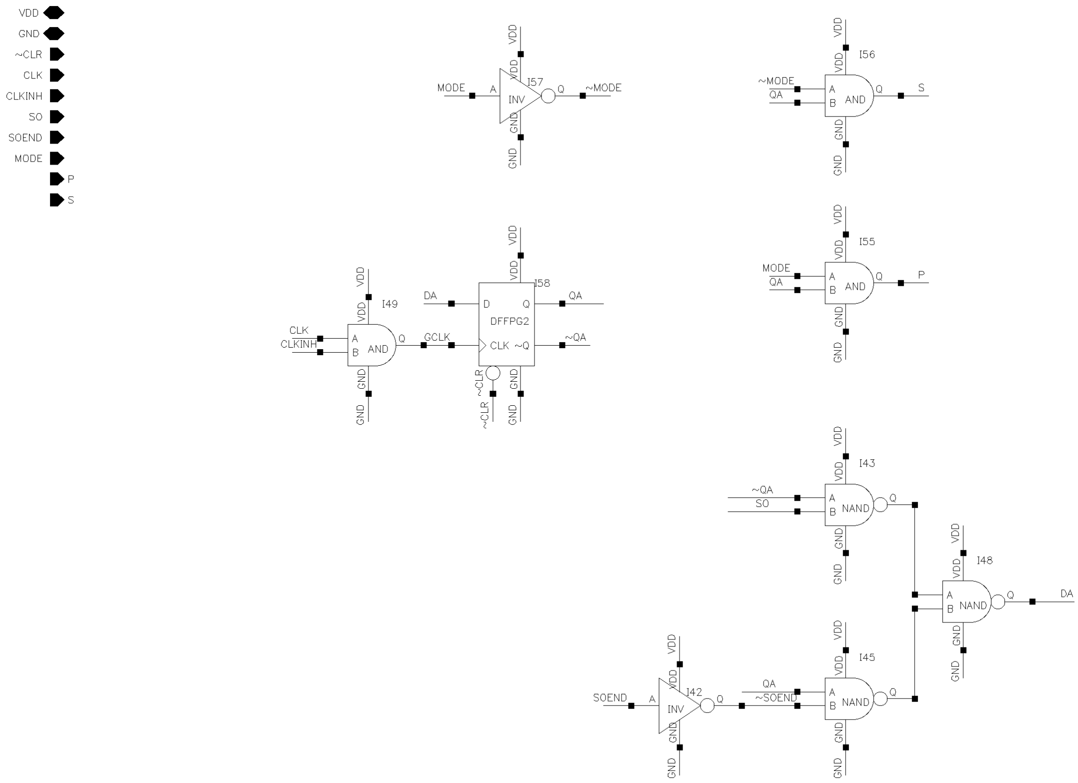


Figure A.11: Schematic of the Readout Controller

Appendix B

Perl Code for Data Processing

B.1 Example Code for Extracting IDs from Monte Carlo Simulation Results in ADE XL

```perl
use feature 'say';
use strict;
use warnings;

# Constants
my $ID_LENGTH = 64;

# Subroutines
sub  trim { my $s = shift;
$s =~ s/^\s+|\s+$//g;
return $s };  # Referred to http://perlmaven.com/trim

# Filenames
my $f_result = "BAPOST30.txt";
my $f_idout = "ID_OUT.txt";
my $f_unique = "ID_UNIQUE.txt";
my $f_uniform = "ID_UNIFORM.txt";

# Extract produced IDs
open(RESULT, $f_result);
open(OUT, ">", $f_idout);

my $bitCount = 0;
my @ID;
my $row_counter = 0;
while(my $line = <RESULT>)
{
        if($line =~ "VT")
        {
                my $temp = trim($line);
                my @sp = split(/ /, $temp);
                my $value = trim($sp[4]);

                if($value < 2.5)
                {
                        #print 0;
                        push @ID, 0;
                }
                else
                {
                        #print 1;
                        push @ID, 1;
                }
        $bitCount += 1;
        }

        if ($bitCount == $ID_LENGTH)
        {
                #say @ID;
                say OUT @ID;
                @ID = ();
                undef @ID;
                $bitCount = 0;
                $row_counter += 1;
                say $row_counter;
        }

}
close(RESULT);
close(OUT);
say "Extracting produced IDs......OK";

# Calculate uniformity
open(ID_IN, $f_idout);
open(UNIFORM_OUT, ">", $f_uniform);

while(my $line = <ID_IN>)
{
        my $sum = 0;
        my $temp = $line;
        chomp($temp);
        my @ID = split(//, $temp);
        #say @ID;
        for my $bit (@ID)
```

```
    {
        $sum += $bit;
    }
    say UNIFORM_OUT $sum/$ID_LENGTH;
}


close(ID_IN);
close(UNIFORM_OUT);
say "Calculating uniformity......OK";
```

B.2 Example Code for Computing Uniqueness with Extracted IDs

```
use feature 'say';
# Constants
my $ID_LENGTH = 64;

# Subroutines
sub HD
{
    my $sum = 0;
    my ($arg1, $arg2) = @_;
    my @ID1 = @{$arg1};
    my @ID2 = @{$arg2};
    for(my $iter = 0; $iter < $ID_LENGTH; $iter = $iter + 1)
    {
        $sum += ($ID1[$iter] xor $ID2[$iter]);
    }
```

```
        return $sum;
}

# Filenames
my $f_result = ”Bit16Results.txt”;
my $f_idout = ”ID_OUT.txt”;
my $f_unique = ”ID_UNIQUE.txt”;
my $f_uniform = ”ID_UNIFORM.txt”;

# Calculate uniqueness
open(ID_IN, $f_idout);
open(UNIQUE_OUT, ”>”, $f_unique);

my @ID_MATRIX;
my $row_counter = 0;

while(my $line = <ID_IN>)
{
        my $temp = $line;
        chomp($temp);
        my @ID = split(//, $temp);
        for(my $column = 0; $column < $ID_LENGTH; $column += 1)
        {
                $ID_MATRIX[$row_counter][$column] = $ID[$column];
        }
        $row_counter += 1;
}

my $sum = 0;
my $HammingDistance;
for(my $i = 0; $i < 999; $i += 1)
{
        print "i␣=␣$i\n";
        for(my $j = $i + 1; $j < 1000; $j += 1)
        {
                $HammingDistance = HD(\@{$ID_MATRIX[$i]},
                \@{$ID_MATRIX[$j]}) / $ID_LENGTH;
                say UNIQUE_OUT $HammingDistance;
                $sum += $HammingDistance;
        }
}

my $uniqueness = $sum*2/(1000*999);
print "Uniqueness␣=␣$uniqueness\n";

close(ID_IN);
close(UNIQUE_OUT);
```