# Hardware Trojan vulnerability

by

**Xing Cao**

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

Master of Science

Major: Electrical Engineering

Program of Study Committee:
Randall L. Geiger, Major Professor
Degang J. Chen
Meng Lu

Iowa State University

Ames, Iowa

2015

# DEDICATION

To my family

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

## ACKNOWLEDGEMENTS

I would never have been able to finish my thesis without the guidance of my advisor my committee members, my friends and supports from my family.

First, I would like to express my deepest gratitude to my advisor Dr. Randall L. Geiger for his guidance, support, caring and patience on my research. As a mental, he show me another world of academia and provide me with a wonderful journey in this world. I have benefitted in school and in everyday life from the words he spoke to me.

I would also like to thank my committee members for their guidance and encouragement: Dr. Degang Chen and Dr. Meng Lu. In last several years, they help me to develop my background in integrated circuit and semiconductor materials.

I would like to thank Rui Bai, who gave me suggested and was a great help in my M.S. years. Without her advice, I would have spent many more hours on my research and coursework. In addition, I would like to express my thanks to Tim Hibbing, Rebecca Riker, Qianqian Wang, Zhiqiang Liu, Yifei Li, You Li, Yen-Ting Wang and my other friends, colleagues and anyone who helped me with various aspects of conducting this M.S. works.

Finally, thanks to my parent: Bin Cao and Wuyan Zhou, for giving birth to me and supporting me spiritually throughout my life. They always tell me the truth in the real life and help me to build positive attitude toward my life. Lots of suggestions are influencing me through my whole life.

## ABSTRACT

Many basic analog blocks and structures, which contain positive feedback loops, are vulnerable to the presence of one or more undesired stable equilibrium points. The phenomena of multiple equilibrium points is investigated with emphasis on using a temperature-domain representation to identify equilibrium points in some circuits that have a single positive feedback loop. By example, it is shown that the presence of multiple equilibrium points can often be observed as hysteresis in a plot of an output circuit electrical variable versus temperature obtained from a bidirectional temperature sweep over a temperature interval $[T_1, T_2]$ of interest. The hysteresis can be associated with a relationship comprised of a single continuous locus of points or comprised of two or more disjoint continuous loci of points. The concept of an "isolation region" that can occur in the temperature transfer characteristics of a circuit is discussed where an "isolation region" in the closed interval $[T_1, T_2]$ is defined as any continuous locus of points in $\mathbf{R}^2$ that forms a closed path and that does not include either of the temperature interval endpoints, $T_1$ or $T_2$ . Challenges of determining the presence or absence of multiple stable equilibrium points with standard approaches to simulation and mixed-signal verification will be discussed. Vulnerability of circuits to analog hardware Trojans where the location and size of the hysteresis window can be engineered to serve as a Trojan trigger will be addressed. Concern associated with exploitation of an isolation region as a method for embedding and triggering analog hardware Trojans that are extremely difficult to detect will be raised.

Keywords— Positive Feedback Loop; Hardware Trojan; Isolation Region; Inverse Widlar circuit; Wilson circuit

# CHAPTER I

# INTRODUCTION

The Information Technology (IT) industry has experienced dramatic developments in the last two decades. Due to the widespread use of electronic devices in the IT industry, both electronic hardware and software now play a critical role in human society. They enhance quality of life through the variety of products the technology enables. As computer systems become increasingly threaded in people's lives through entertainment, health care, business, finance, defense, and transportation, reliability and security issues have arisen and are of growing importance.

Currently, Cyber-attacks are common and often spread Trojans that adversely influence our daily life. As portrayed in movies, Trojans may initiate abhorrent incidents like air crashes, financial crises, or even modern wars but much more commonly they cause aberrations in system performance or denial of service which are both annoying and costly. Various types of Hardware Trojans are discussed in this chapter including places where known types of Trojans are vulnerable for inserting and current methods that have been proposed for detecting Hardware Trojan.

## 1.1 Threat from Hardware Trojan

A hardware Trojan is generally defined to be a malicious modification of circuitry and can occur at the system level, at the printed circuit board level, or internal to an integrated circuit [1]. On rare occasion, well-intentioned engineers can make a mistake or have an oversight during the design process that is not malicious but that results in undesired consequences like those associated with malicious modifications. I will also classify these mistakes or oversights as Trojans. In contrast to software Trojans that often cause a denial of service, steal proprietary data, cause

annoying pop-ups, delete or alter files, or create back doors, hardware Trojans often derange or destroy entire integrated circuits or components in addition to causing a denial of services. In general, software Trojan can often be mitigated or removed by deleting or removing the Trojan files. In contrast, hardware Trojans present in a system will invariably exist indefinitely in the system hardware.

Today, with the development of the IC industry, people are relying heavily on “smart” electronic devices, which are based on integrated circuits. Powerful IC chips, the virtual brain for all electronics, are influencing our life and release us from repeatable and boring tasks, but they also introduce potential risks that can be exploited by hackers or other adversaries. Throughout the remainder of this thesis, hackers or other adversaries that exploit system vulnerabilities to intentionally and negatively impact performance will be termed the “bad guys”.

As a worldwide change is occurring in where integrated circuits are manufactured, tested, and distributed, both the military and the commercial sectors are concerned about whether electronic devices and systems can be trusted. Counterfeit electronic components are rampant in the microelectronics supply chain, and those responsible for procuring semiconductor components and maintaining cyber, military, financial, and other critical systems are extremely concerned about insertion of hardware and software Trojans into components and systems through the counterfeit component supply chain [2].

Since hardware Trojans can be readily hidden within an integrated circuit, and since they have the powerful ability to either alter circuit performance or destroy the integrated circuit, it is difficult to imagine the terrible incidents that can occur if terrorists are able to insert hardware Trojans in critical integrated circuits. As an example, imagine a situation where “bad guys” have inserted a hardware Trojan into the control system of a commercial airliner that has been designed

so that all the terrorists need to do to trigger the Trojan is to push a button and when the button is pushed, all electrical system of the plane will fail or shut down. This electrical system failure could cause the aircraft to crash and kill all aboard. Undoubtedly, threat from hardware Trojans will become of increasing concern as the volume of integrated circuits increase and as the design, production, and distribution supply chain becomes more distributed and diverse throughout the world.

### 1.2 More detail about inserting Hardware Trojan

Integrated Circuit (IC) design companies and manufacturers increasingly rely on untrusted parties and entities through the entire IC development, procurement, deployment and utilization life cycle. Economic factors including cost of labor and governmental subsidization or support to the semiconductor industry in different countries have created a semiconductor industry in which most of the modern ICs are manufactured in unsecured fabrication facilities. Furthermore, untrusted third-party vendors and outsourced design and test services throughout the semiconductor industry now provide intellectual property (IP) cores [3] that are an integral part of otherwise trusted designs. Thus there are many points throughout the semiconductor supply chain where hardware Trojans can be inserted into integrated circuits.

A flowchart that shows a typical IC design and fabrication cycle is shown in Fig.1 [4]. The design flow has been grouped into four main functional blocks: design, layout, verification and fabrication. Design represents the first four steps in the flowchart. Layout represents physical design. Verification represents physical verification and signoff. I am not concerned about the processing steps after fabrication since hardware Trojans will invariably exist indefinitely in the system hardware once a chip is fabricated. In those four major blocks, I also assume all untrusted

third-party vendors can participate and "bad guys" may or may not exist in those untrusted third-party vendors.

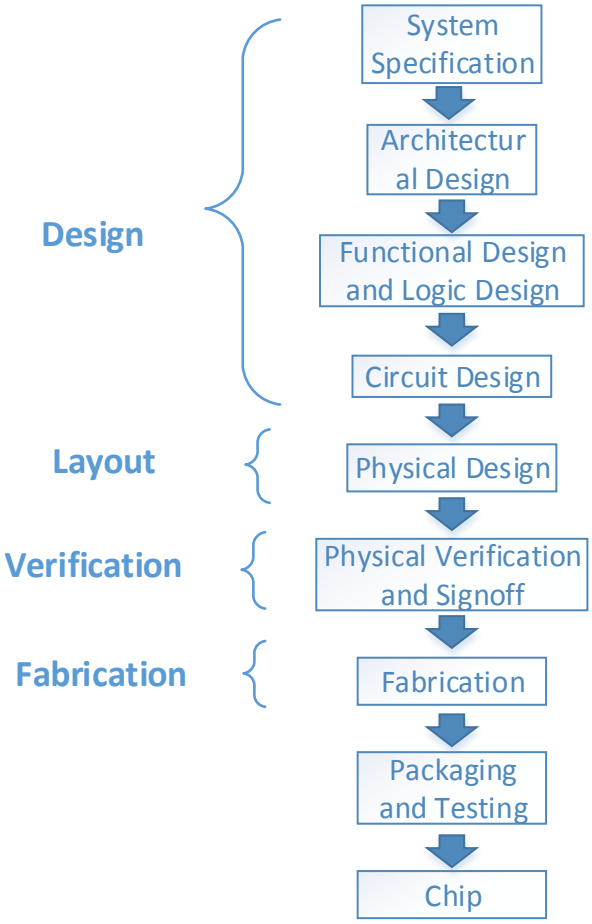



Figure 1. Flowchart of IC producing

### 1.3 Existing methods for Hardware Trojan detection

Tehranipoor published a survey of hardware Trojan taxonomy and detection [5]. In his survey, he identified three methods for detecting hardware Trojans. These three methods are based upon

1) Side Channel Signal Analysis
2) Evidence of Trojan Activation
3) Evidence of Architectural Tampering.

The analysis of side channel signals, primarily timing and power, can be used for Trojan detection. These are descriptively termed Power-Based Analysis and Timing-Based Analysis. The authors of [6] discussed utilizing the side-channel information to detect the contribution of power consumption from the Trojan. The authors discussed the "extra" signal provided by side-channel information such as power consumption, noise and other power-related phenomena caused by an inserted Trojan.

The authors in [7] discussed the use of Timing-Based Analysis. The authors claim that a delay-based side-channel analysis similar to that used for authentication with physical unclonable functions (PUF) can be adapted for hardware Trojan detection however they specifically point out that "a well-hidden HTH (Hardware Trojan Horse) (that) acts fast when sprung at run time ….. will most likely go undetected" by their approach.

Although these methods can be used to detect some hardware Trojans, both approaches require golden models or sets of golden chips that can be used to characterize the desired performance. "Gold models" and "golden chips" refer to models or chips that do not harbor a Trojan. These hardware Trojan detection methods have some serious limitations. First, the aberrations in performance introduced by the Trojan must be of sufficient magnitude to be distinguishable from normal PVT variations. Second, a Golden circuit may not exist if the design process is producing a single design. Third, it may not be easy to trigger a Trojan at test if it is unknown whether a Trojan exists or not or, even if it were known that a Trojan exists, it may not be easy to trigger the Trojan during verification or test for the purpose of locating where it occurs.

The second identified detection method is based upon evidence of Trojan activation. The main concept for this method is to observe aberrations in activity when the Trojan is activated to determine whether there is or is not a Trojan. The authors of [8] use random inputs in an attempt

to active the Trojan hidden in the circuit. A difference in outputs from what is expected is evidence of the presence of a Trojan.

In [9], the author provide another method for utilizing the evidence of Trojan activation. In contrast to the work in [8] where the emphasis was placed only upon input/output relationships for the entire system, the author localized the region in which to look for the effects of a Trojan with the argument that focusing on localized excitation and localized response offers potential for increasing the difference between the ideal and compromised responses.

The methods of Trojan activation could combine with Side Channel Signal Analysis and be an assistant tools to accelerate the testing speeding. However, either "picking random inputs" or "defining the potential Trojan inserted area" may not be efficient ways for determine the location of well-hidden Trojans. With increasing numbers of transistors, these methods can become extremely time-consuming.

Finally, it is Architecture Level Trojan detecting. Design abstraction can be clarified with different levels like protocols, software, micro-architecture, and circuits. Architecture Level Trojan divides a system into different levels and defines key factors like power consumption for each different structure at first. During detecting process, Trojan can be determined by comparing the actual key factors with the data defined before. Like [10], the authors propose a special checksum to verify the inserted Trojans by checking the performance of hardware in a low level. Only certificated hardware can obtain a fast speed by using this checksum so we can determine the Trojans by comparing the different performance.

To demonstrate the idea above, it still need "certificated hardware", which is unrealistic in IC designing process. Also, comparing every detail becomes impossible with increasing number of transistors and much complicated architecture design.

## 1.4 Research Motivation

Current economic trends are one of the key factors reinforcing the vulnerability to Trojan attacks. With increasing reliance on untrusted third-party vendors, security concerns have risen to unprecedented levels and hardware Trojans have become a major threat in the IC industry. Unlike software Trojans, a hardware Trojan is almost impossible to remove from a chip after fabrication. The impact of embedded hardware Trojans can be devastating. Hardware Trojans can cause a circuit or system to enter an undesired operating state, can trigger a release of private information, can cause a system to fail, can cause an integrated circuit to self-destruct, or possibly even give control of a system to an adversary. Therefore, it is critical to develop methods for identifying or revealing hardware Trojans before fabrication to avoid the costly or devastating effects of an undetected Trojan.

A clever attacker will attempt to hide or disguise Trojans in a way that makes it extremely difficult to detect with conventional verification and testing. This could include designing trigger mechanisms that will only trigger the Trojans under rare conditions.

One class of hardware Trojans that have received very little attention are those associated with the analog circuitry in an integrated circuit. The area has received so little attention that a taxonomy of different classes of analog hardware Trojans has not yet evolved. In spite of the fact that analog hardware Trojans have not received much attention, they can be easily embedded into many integrated circuits and their impact can be insidious. One type of analog hardware Trojans is those associated with the presence of one or more undesired equilibrium points whereby the undesired equilibrium points can be classified as Trojan states.

In this thesis, characteristics of analog circuits with multiple equilibrium points in a circuit with single positive feedback loop are investigated. It has been shown that the existence of one or

more positive feedback loops is a necessary condition for the presence of a Trojan operating state. Trojan operating states can be very difficult to detect because existing simulation and verification tools naturally provide only a single solution with no provisions for determining more than one stable equilibrium point if it or they are known to exist. Circuits with more than one operating point often exhibit some unique performance in the temperature-domain and this temperature-domain performance can often provide insight into the presence of more than one equilibrium point. In this thesis, the temperature-domain performance of circuits that may have more than one equilibrium point is investigated.

The intriguing behavior of circuits with multiple equilibrium points has inspired me to study circuits with a potential hardware Trojan vulnerability that escapes detection with most existing detection methods. In this research on the temperature-domain behavior of circuits with multiple equilibrium points, I reveal the existence of an isolation region in the temperature transfer characteristics of the Wilson current mirror circuit and develop a deeper understanding of the isolation region in the Inverse Widlar circuit. A systemic approach for finding the presence of the isolation region in the Wilson circuit is discussed whereby the isolation region in the Inverse Widlar circuit is morphed into an isolation region in the Wilson circuit using a circuit-based continuation approach. In a prototype circuit, methods for controlling the location and shape of the isolation region are discussed.

# CHAPTER II

# MULTIPLE EQUILIBRIUM POINTS

A circuit with static biasing and no time-varying inputs that has more than one DC operating point is said to have multiple equilibrium points. If the circuit is designed to have a single operating point but the circuit actually has more than one stable equilibrium point, the circuit is plagued by the multiple equilibrium point problem since a circuit can maintain static operation at any stable equilibrium point irrespective of whether the equilibrium point is a desired operating point or a Trojan operating state. Many widely used circuits that have one or more positive feedback loops are known to be vulnerable to the presence of multiple equilibrium points. Most temperature sensor and reference generator circuits use one or more positive feedback loops to reduce output sensitivity to the power supply voltage and these circuits are vulnerable to the multiple equilibrium point problem [12]. Circuits with multiple equilibrium points exhibit different performance between the voltage-domain and the temperature-domain. I will focus on temperate-domain characteristics of circuits with multiple equilibrium points throughout the remainder of this thesis.

## 2.1 The definition of equilibrium point

The “resistive” circuit of a nonlinear circuit is the circuit that is obtained by removing all energy storage elements by replacing all capacitors with open circuits and all inductors with short circuits. An equilibrium point of a nonlinear circuit with static bias and static excitation is a solution of the “resistive” circuit of the nonlinear circuit. A nonlinear circuit is said to have multiple equilibrium points at a temperature T if the resistive circuit has more than one solution under the same static bias and static excitations. All linear circuits under static bias and excitation

conditions will have a single equilibrium point. A nonlinearity is a necessary but not sufficient condition to cause the presence of multiple equilibrium points.

Any equilibrium point of a nonlinear circuit under static bias and static excitation conditions can be classified as either a stable equilibrium point or an unstable equilibrium point. An equilibrium point of the resistive circuit of a nonlinear circuit with static bias and static excitation is a stable equilibrium point if

a) there exists a set of initial conditions for all of the energy stored elements of the circuit that will cause the transient response of the circuit to remain at the equilibrium point
b) there exists a small neighborhood around the set of initial conditions described in part a) such that if initial conditions in this neighborhood are established, the transient response of the circuit will converge to the same equilibrium point

An equilibrium point of a resistive circuit under static bias and static excitation that is not a stable equilibrium point is said to be an unstable equilibrium point. If a circuit has one or more undesired stable equilibrium points, the undesired stable equilibrium points will termed Trojan states or Trojan operating points.

## 2.2 Circuits with Multiple Equilibrium Points

In this section, examples of circuits that have multiple equilibrium points will be discussed. It is well known that all of the circuits shown in Fig. 2 and Fig. 3 are vulnerable to the presence of multiple stable equilibrium points. More specifically, for some implementations of these circuits in some semiconductor processes, the circuits will possess two or more stable equilibrium points.

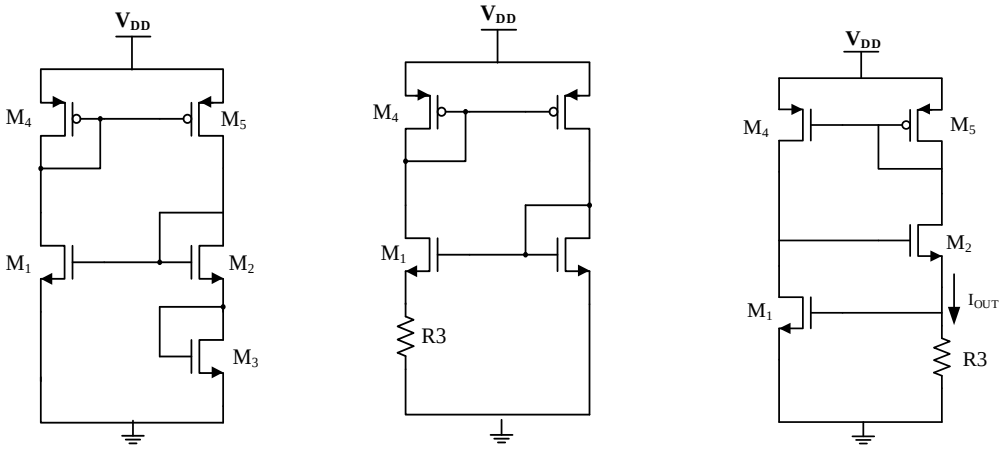



Figure 2. Single positive feedback loop (Inverse Widlar, Widlar, Wilson)

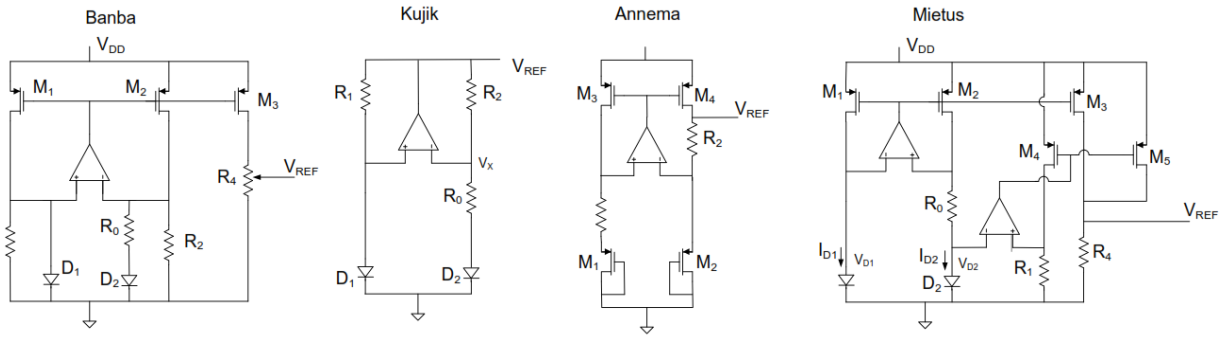



Figure 3. Four popular single DC positive feedback

The three basic circuits shown in Fig.2 [13, 14] have a single positive feedback loop. In different design, these circuits can be utilized as bias generators, current references, voltage references, or temperature sensors. Correspondingly, the four popular circuits shown in Fig.3 [15, 16, 17, 18] each have a single positive feedback loop and are widely used as voltage references. These will be used as initial benchmark circuits for identifying the stable operation points in single positive feedback loop circuits.

### 2.3 Methods of detecting multiple equilibrium points

There are many papers that can be found in the literature for determining operating points of circuits. Topology methods using a graphical representation and some topological criteria for identifying multiple equilibrium points are discussed by the authors in [19]. Based on piecewise-linear approximations of all nonlinear devices, piecewise-linear methods were used to provide all operating points of a circuit [20, 21]. In other works, continuous/homotopy methods have been used to track DC solutions [22]. In [23], a break-loop homotopy method was proposed and it finds all stable operating points for CMOS circuits with one positive feedback loop by breaking the positive feedback loop in the circuit at the gate of a transistor, inserting a voltage source at the break point, and sweeping the voltage to create a return map. From the return map, the stable equilibrium points can be obtained. In [24, 25, 26], SAT and/or SMT-based formal methods are discussed that can be used to obtain equilibrium points.

These methods are alternatives for finding all the operating points of a nonlinear circuit. This continues to be a very challenging problem. Some of these methods can only provide partial solutions. Some can be used to obtain complete solutions at the expense of requiring significant computation time.

# CHAPTER III

# TEMPERATURE-BASED METHODS FOR TROJAN DETECTING

In this chapter, two temperature-based methods that can be used for detecting the presence or absence of Trojan states for some circuits will be discussed. One is based upon a bi-directional temperature sweep and the other is based upon obtaining temperature transfer characteristics using a node-set at each point in the temperature domain. In the bi-directional sweep method, a resultant hysteresis window is indicative of a circuit having a Trojan state. The concepts of hysteresis windows and isolation regions in the temperature transfer characteristics, which are two specific types of behavior that can occur in circuits with multiple equilibrium points, will be discussed. Finally, a special phenomenon that can occur when using a standard circuit simulator to determine the temperature transfer characteristics, which I have termed "shaking" will be presented. The "shaking" phenomena can also be useful for identifying the presence of multiple equilibrium points in a nonlinear circuit.

The presence of multiple equilibrium points can often be observed as a hysteresis window in a plot of a circuit variable, specifically a voltage or current in the circuit, versus temperature obtained from a bidirectional temperature sweep over a temperature interval $[T_1, T_2]$ of interest. An "Isolation region", which will be defined formally in this section, is conceptually any continuous closed locus of points that forms a loop in the relationship between a circuit variable and temperature that is separated by a finite distance from all other points in the relationship on the temperature interval $[T_1, T_2]$.

### 3.1 Temperature sweep methods

For the purpose of determining whether an analog circuit has more than one stable equilibrium point [27], two simulation methods based upon temperature sweeps will be discussed. One involves a bi-directional temperature sweep [28] and the other a "node-set" based sweep. Both are computationally efficient and have been effective at finding multiple equilibrium points in quite a few benchmark circuits though we can't guarantee these methods will find all operating points in all circuits.

One of my classmates first observed that a bi-directional temperature sweep often exhibits the presence of a hysteresis region. With further study of operating points, another method called the "node-set" method has been found to show the presence of multiple equilibrium points when they exist even if the bi-directional sweep fails.

#### 3.1.1 Bi-directional temperature sweeping

The bi-directional temperature sweeping is a method to obtain the node voltage from a bidirectional temperature sweep with a standard circuit simulator over a temperature interval $[T_1, T_2]$. By applying this method, the temperature is swept from both directions, that is, it is sweep from $T_1$ to $T_2$ and from $T_2$ to $T_1$. For example, in the Inverse Widlar circuit of Fig.4, the node voltage of interest could be set at the gate of either M1 or M4 and then the temperature could be swept in both directions through the interval $[T_1, T_2]$. The simulation results shown in Fig.5 (a) were obtained from a bi-directional temperature sweep for the inverse Widlar circuit. The simulation result show the output voltage of node A. The process used is the AMI 0.5 μm process. The device sizes and supply voltage used in the simulation are given in Table 1. From this simulation, it can be observed that there are at least two equilibrium points in the hysteresis window from T=52$^{o}$C to T=188$^{o}$C.

Table 1. Simulation environment (1)

| | | | |
|---|---|---|---|
| Technology(process) | AMI 0.5 µm | M1(W/L/M(multiplier)) | 4.5 µ/1.8 µ/5 |
| Supply voltage | 5V | M2(W/L/M(multiplier)) | 4.5 µ/1.8 µ/5 |
| Output node | A | M3(W/L/M(multiplier)) | 1.5 µ/4.05 µ/1 |
| Structure | Inverse Widlar | M4(W/L/M(multiplier)) | 1.5 µ/1.2 µ/8 |
| | | M5(W/L/M(multiplier)) | 1.5 µ/1.2 µ/8 |

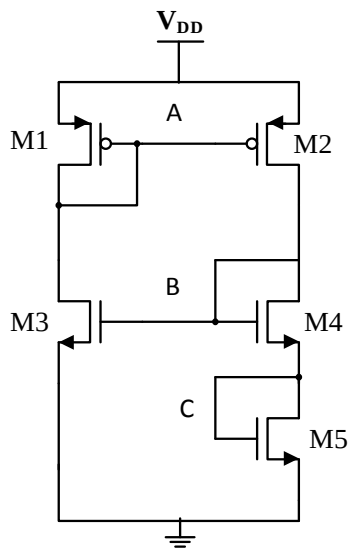
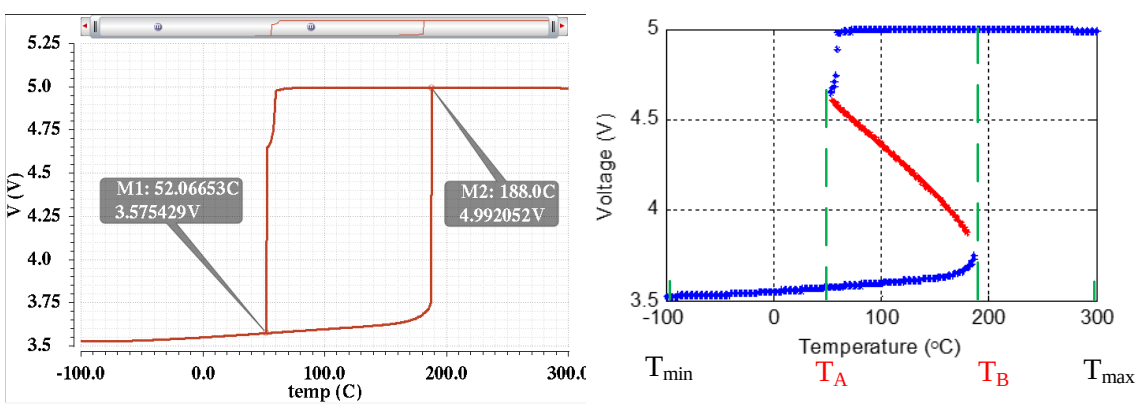



Figure 4. Inverse Widlar Circuit




(a) (b)

Figure 5. Simulation results for Inverse Widlar Circuit, (a) from bi-directional sweep (b) actual transfer characteristics

With the temperature sweep in a standard circuit simulator, the previous simulation result serves as the initial condition for the next simulation, which means each simulation step in the temperature hysteresis sweep method is related to the immediately preceding simulation step. Depending on the temperature interval and actual behavior of multiple equilibrium points, it may or may not miss the multiple equilibrium points. It should be noted, however, that the hysteresis sweep does not give all equilibrium points. The actual transfer characteristics for this circuit are shown in Fig. 5(b). It can be noted from this figure that this circuit has three operating points in the temperature interval from T=52$^{o}$C to T=188$^{o}$C. The ones identified by the hysteresis sweep are the stable equilibrium points. The intermediate points that are on the portion of the transfer characteristics with negative slope are unstable equilibrium points. Simulation of the unstable equilibrium points is often a tedious process and will not be discussed in this thesis.

Though the simulation results shown were for the node voltage $V_A$, the hysteresis would be present for any node voltage, any branch current, or any branch voltage so it is not critical which electrical variable is used for the bidirectional sweep.

### 3.1.2 "Node-set" method

The "Node-set" method is another method to track the node voltage by doing simulations with a standard circuit simulator over a temperature interval of interest. With the "node-set" method, users set the initial condition for each simulation first. Then a parametric analysis is applied and simulations are made at temperatures through the interval $[T_1, T_2]$. By setting initial conditions close to an actual solution, the simulations will often be attracted to a particular solution.

In contrast to the bi-directional temperature sweep method, simulation at each temperature with the "node-set" method is independent from other simulations. Thus, it makes no difference on which order the individual temperature simulation points are chosen. If a node has been set

before using this parametric analysis sweeping method, then every simulation at each temperature will start from this same node set. Though it may appear that the "node-set" method eliminates half of the simulations compared to that required for bidirectional sweeping, the simulation times required using the "node-set" method are often much longer for several reasons. One is the time required for convergence in individual simulations. Since the results of the previous simulation do not serve as initial conditions, the time for each simulation may be much longer. But the major reason that the "node-set" approach may be quite time consuming is because there is often no good way to determine initial conditions that will result in convergence to multiple equilibrium points. And, the initial condition vector can be of high dimension further complicating the task of determining a good set of initial conditions. However, in examples that have been investigated, the "node-set" approach has been useful at determining multiple equilibrium points in some circuits.

As an example, the "node-set" method has been used with three different node-settings of node A in the inverse Widlar circuit of Fig. 4 using the Spectre circuit simulator. The process used for these simulations is the AMI 0.5 μm process. The device sizes, supply voltage and node-setting voltage for each simulation are given in Table 2. The node set was made only at node A with default initial conditions being used at the other nodes. Results from the simulation that show the loci of multiple equilibrium points for the voltage on Node A are shown in Fig.6. In these simulation results the colors green, red and blue are used to show the results under the different node-setting conditions. Though it may appear that for temperatures below 59$^{o}$C or above 102$^{o}$C there is only one simulation result, simulation results for all three initial conditions were identical in these lower and upper temperature regions and the plotting routine I used only displays one color, in this case blue, in these regions.

From this simulation, it can be observed that there are at least three equilibrium points from $T_1$ =59.18°C to $T_2$ =102°C. Also, we find that there is a region which is a continuous locus of points in $\mathbf{R}^2$ that forms a closed path and that does not include either of the temperature interval endpoints, $T_1$ or $T_2$ . We call this region as "isolation region", which will be discussed later. Though the "node-set" method can be quite time consuming, other methods often fail to determine the presence of multiple solutions when an "isolation region" exists.

Table 2. Simulation environment (2)

| | | | | | |
|---|---|---|---|---|---|
| Technology(process) | AMI 0.5 µm | M1(W/L/M) | 3 µ/3 µ/5 | Green | 4.9V |
| Supply voltage | 5V | M2(W/L/M) | 3 µ/3 µ/5 | Red | 4.0V |
| Output node | A | M3(W/L/M) | 1.5 µ/3 µ/1 | Blue | 3.5V |
| Structure | Inverse Widlar | M4(W/L/M) | 110 µ/1.8 µ/8 | | |
| | | M5(W/L/M) | 3 µ/600n/1 | | |

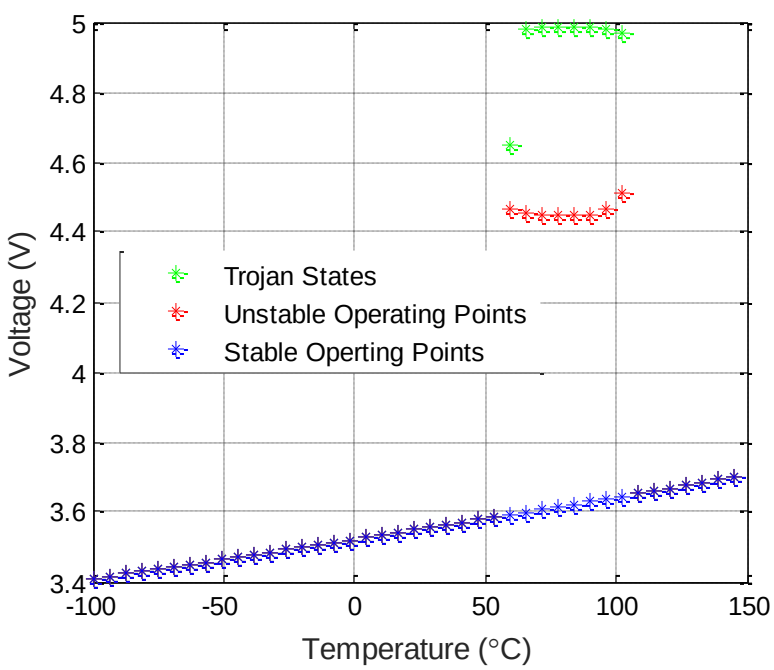



Figure 6. Loci of multiple equilibrium points (an isolation region)

### 3.2 Definition of hysteresis window

Though a hysteresis window was observed in the simulation results shown in Fig. 5 (a), the definition of a hysteresis window was not formally defined. We say a relationship $f(T)$ exhibits a Hysteresis window in the interval $[T_{1min}, T_{2max}]$ if a bidirectional temperature sweep shows that it has at least two solutions in this interval and is single valued for $T < T_{1min}$ and single valued for $T > T_{2max}$.

Bi-directional sweeping of the temperature from low temperature to high temperature and from high temperature to low temperature is often a practical method for observing the presence of a hysteresis window. The general representation of a bi-directional temperature sweep that exhibits a hysteresis window in the interval $[T_1, T_2]$ is shown in Fig.7. An example of a hysteresis window in the interval [52$^o$C, 188$^o$C] was shown in Fig.5 obtained from a bi-directional temperature sweep for a specific implementation of the Inverse Widlar circuit.

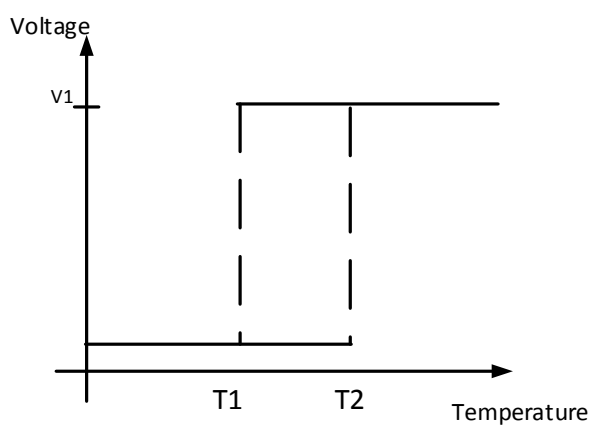



Figure 7. The rough description of hysteresis window

### 3.3 Definition of Isolation Region

The transfer characteristic of a real valued relationship $f(T)$ on the interval $[T_A, T_B]$ is said to have an isolation region if

(1) $f(T)$can be represented as the union of two continuous relationships $f_1(T)$ and $f_2(T)$ where $f_1(T) \cap f_2(T) = \emptyset$

(2) $\exists\ \epsilon\ > 0$ such that $|f_1(T_1) - f_2(T_1)| > \epsilon,\ \forall\ T_1 \in [T_A, T_B]$

(3) Domain of $f_1(T)$ is a proper subset of $(T_A, T_B)$

The simulation results for an implementation of the Inverse Widlar circuit shown in Fig.6 exhibit the presence of an Isolation Region.

An isolation region is one kind of behavior that can be exhibited with circuits that have multiple equilibrium points in the temperature domain. To my knowledge, the existence of isolation regions had not been reported in the literature though a fellow classmate, Qianqian Wang, recently submitted a paper for review, [28], that discusses the concept of an isolation region. Isolation regions may or may not be readily detected from a bi-directional temperature sweep. The existence of isolation regions in the Inverse Widlar structure were discovered by chance when exploring the temperature characteristics of the circuit with bi-directional temperature sweeps and perturbations of the circuit in an attempt to control the characteristics of the hysteresis window. The following figures describe the evolution of an isolation region.

Consider a circuit with the “S” shape transfer characteristics indicative of multiple equilibrium points shown in Fig.8 (a). These characteristics are based on the inverse Widlar circuit of Fig. 4 designed in the AMI 0.5 µm process. The vertical axis is the voltage on Node A in all parts of Fig. 8. The simulation results shown in Fig.8 (b), (c), (d), (e), (f)] depict the evolution

of an isolation region as the width of transistor M5 is changed. Here, each figure contains three simulation results (shown with green, red and blue dots) under different node-setting voltages. The supply voltage and node-setting voltage for node A used in these simulations are given in Table 3 and the size of all transistors are given in Table 4. Default values in the circuit simulator were used for all other node set voltages. It should be noted that the isolation region can be substantially isolated form the remainder of the transfer characteristics as can be observed in the plot of Fig. 8 (f).

Table 3. Simulation environment (3)

| | | | |
|---|---|---|---|
| Technology(process) | AMI 0.5 μm | Green | 4.9V |
| Supply voltage | 5V | Red | 4.0V |
| Output node | A | Blue | 3.5V |
| Structure | Inverse Widlar | | |

Table 4. Simulation environment (4)

| Transistor | Size(a) (W/L/M) | Size(b) (W/L/M) | Size(c) (W/L/M) | Size(d) (W/L/M) | Size(e) (W/L/M) | Size(f) (W/L/M) |
|---|---|---|---|---|---|---|
| M1 | 3μ/3μ/5 | 3μ/3μ/5 | 3μ/3μ/5 | 3μ/3μ/5 | 3μ/3μ/5 | 3μ/3μ/5 |
| M2 | 3μ/3μ/5 | 3μ/3μ/5 | 3μ/3μ/5 | 3μ/3μ/5 | 3μ/3μ/5 | 3μ/3μ/5 |
| M3 | 1.5μ/3μ/1 | 1.5μ/3μ/1 | 1.5μ/3μ/1 | 1.5μ/3μ/1 | 1.5μ/3μ/1 | 1.5μ/3μ/1 |
| M4 | 110μ/1.8μ/1 | 110μ/1.8μ/1 | 110μ/1.8μ/1 | 110μ/1.8μ/1 | 110μ/1.8μ/1 | 110μ/1.8μ/1 |
| M5 | 9μ/600n/1 | 6.8μ/600n/1 | 6.7μ/600n/1 | 6.65μ/600n/1 | 6.5μ/600n/1 | 3μ/600n/1 |

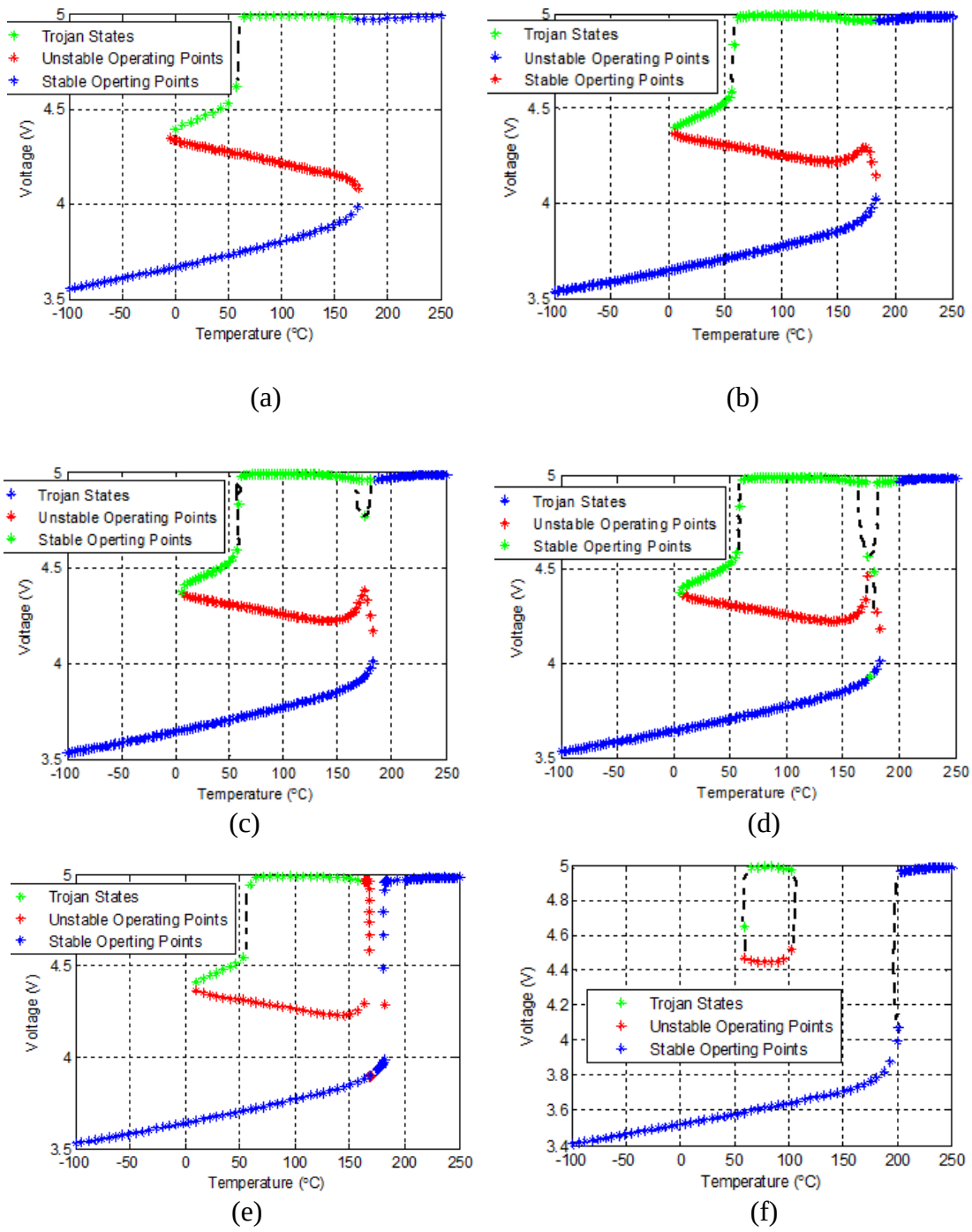



Figure 8. Evolving of isolation region

In an attempt to see how sensitive the isolation region location and shape are to a particular process, the same evolution procedure was considered for an implementation of the Inverse Widlar structure of Fig. 4 in an IBM 0.13 μm CMOS process. The evolution of an isolation region in the

IBM 0.13 µm CMOS process is shown in Fig. 9 . In this evolution, only the size of transistor M5 is changed and the output of the voltage of node A was observed. Each part of the figure contains three simulation results (shows in green, red and blue dots) under different node-setting voltages (different initial voltage for of Node A, default initial conditions used for all remaining nodes). The supply voltage and node-setting voltage for Node A are given in Table 5. The size of all transistors used in the simulation are shown in Table 6.

Table 5. Simulation environment

| | | | |
|---|---|---|---|
| Technology(process) | IBM 0.13 µm | Initial $V_A(1)$ | 1.2V |
| Supply voltage | 1.2V | Initial $V_A(2)$ | 1.08V |
| Output node | A | Initial $V_A(3)$ | 0.7V |
| Structure | Inverse Widlar | | |

Table 6. Simulation environment

| Transistor | Size(a) (W/L/M) | Size(b) (W/L/M) | Size(c) (W/L/M) | Size(d) (W/L/M) |
|---|---|---|---|---|
| M1 | 1 µ/600n/60 | 1 µ/600n/60 | 1 µ/600n/60 | 1 µ/600n/60 |
| M2 | 1.2 µ/1.2 µ/1 | 1.2 µ/1.2 µ/1 | 1.2 µ/1.2 µ/1 | 1.2 µ/1.2 µ/1 |
| M3 | 2 µ/600n/1 | 2 µ/600n/1 | 2 µ/600n/1 | 2 µ/600n/1 |
| M4 | 1 µ/600n/1 | 1 µ/600n/1 | 1 µ/600n/1 | 1 µ/600n/1 |
| M5 | 320n/600n/1 | 280n/600n/1 | 230n/600n/1 | 220n/600n/1 |

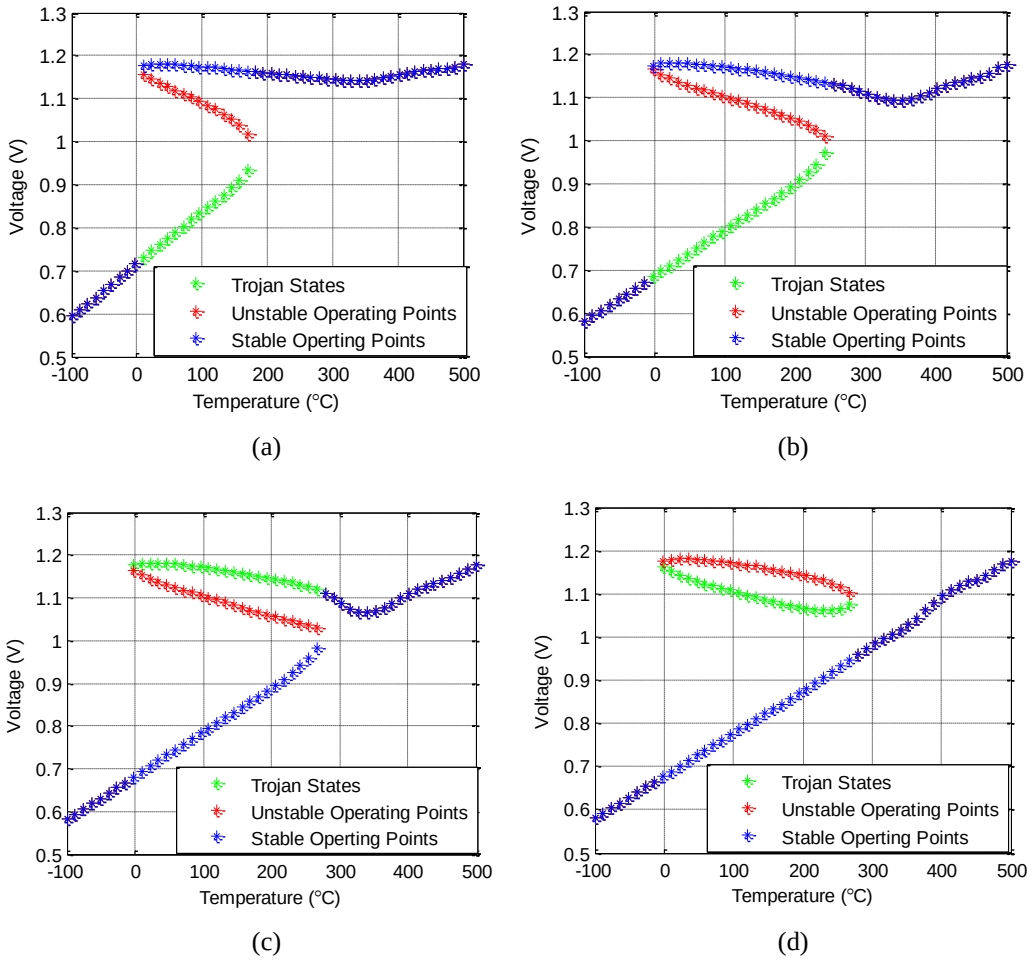



Figure 9. Evolving of isolation region

In this investigation, the isolation regions occurs in a very small subset of the design space for inverse Widlar circuit in the IBM 0.13 μm CMOS process. Since this isolation region occurs over a very small subset of the design space, it may be particularly difficult to detect if its presence is unknown.

The existence of an isolation region has also been found in the Wilson structure and it will be discussed in the following chapter. There may be some particularly useful applications for circuits with isolation regions but considering how difficult it can be to detect the presence of an

isolation region, isolation regions may provide fertile territory for hiding analog hardware Trojans in widely used circuit structures.

### 3.4 "Shaking" phenomena

By using the "node-set" method, we may get different results by applying different initial condition (setting different initial node voltage). Some of these results may, at first glance, appear to be associated with an incorrect use of a circuit simulator and designers may be tempted to ignore the results but as will be seen here, they may provide information about the existence of Trojan states that may not be detected by other methods. Consider a circuit with an isolation region like that shown in Fig.6. By setting different initial voltages, we would expect to obtain results like those shown in Fig.10 (a) and Fig. 10 (b). However, I have also obtained results shown in Fig.10 (c) and Fig. 10 (d) as well for simulations of the Inverse Widlar circuit of Fig. 4.

In Fig. 10, each part of the figure contains one simulation results obtained by using the "node-set" method by using different node-setting voltages for the Inverse Widlar circuit. The output variable in these simulations is the node voltage of node A. The process used is the AMI 0.5 μm process. The size of each transistor, supply voltage and node-setting voltage are given in Table 7.

Table 7. Simulation environment (7)

| | | | | | |
|---|---|---|---|---|---|
| Technology (process) | AMI 0.5 μm | M1(W/L/M) | 3 μ/3 μ/5 | Initial $V_A$(a) | 3.0V |
| Supply voltage | 5V | M2(W/L/M) | 3 μ/3 μ/5 | Initial $V_A$(b) | 4.4V |
| Output node | A | M3(W/L/M) | 1.5 μ/3 μ/1 | Initial $V_A$(c) | 4.9V |
| Structure | Inverse Widlar | M4(W/L/M) | 110 μ/1.8 μ/8 | Initial $V_A$(d) | 4.78V |
| | | M5(W/L/M) | 3 μ/600n/1 | | |

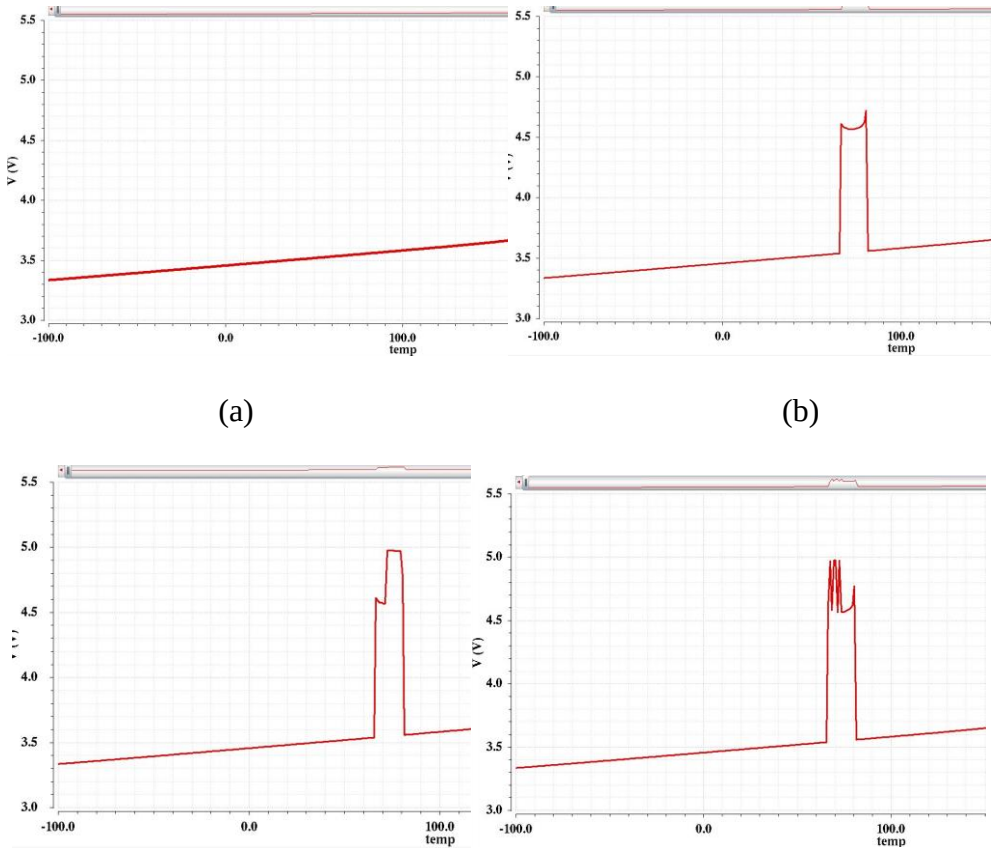



Figure 10. Multiple simulation results

Depending on the value of node set, different simulation results may be generated for circuit with multiple operating states in certain temperature domain. As shown in Fig.10 with different node-setting, the simulation results seem like a smooth continuous line (actually it is continuous loci of points) in Fig.10 (a) and Fig. 10(b), but a “shaking” characteristic is exhibited in the results in Fig.10 (c) and Fig. 10 (d). These results are correct but show convergence to different solutions at closely spaced temperature points. In this case, these somewhat peculiar results may appear to raise questions about the simulation.

The “shaking” phenomena is related to the initial condition voltages set for the simulations and the algorithms used in the Spectre circuit simulator. Since the algorithms in Spectre result in

convergence to an operating point, “shaking” tends to occur if we set the initial condition voltages at values that are between a Trojan state and an unstable operating point. These simulation results enforce the observation that the “node-set” method cannot find all operating points by only setting one initial voltage.

Although the “node-set” method can’t be used to guarantee finding all operating points in the circuit, it is still a useful method for finding the presence of Trojan states and determining the loci of multiple equilibrium points for some circuits.

# CHAPTER IV

# ISOLATION REGION IN DIFFERENT PROCESS AND STRUCTURE

Isolation region is an interesting phenomenon and it has different performance between different structures and different processes. According to the simulation result, it is shown that the center location of isolation region will be fixed when we minimum the size of temperature interval of isolation region range under AMI 0.5μm process. However, it is also found that both width and location of isolation region are changeable under IBM0.13 process. In addition, isolation region not only happens in inverse Widlar circuit, but also exits in Wilson circuit.

## 4.1 The performance of Isolation Region under AMI 0.5μm Process

Initially, it plans to change the size to rearrange the temperature range and location so that it can be either temperature trigger or Trojan circuit. When it randomly changes the size of each

transistor, it is found that the location of center-point of isolation region is fix when it minimizes the sizes of isolation region. Minimum sizes of isolation region means the isolation region will disappear if it keep changing the size of each transistor.

Since the target is exploring the performance of isolation region, randomly sizing the transistors is not acceptable and it does have some rules between changing each transistors and isolation region. To investigate the behavior of isolation region thoroughly, it is necessary to understand the relationship between size of each transistor and isolation range, which is difficult to figure out only by monitoring. Therefore, small size analysis is being used here. The main idea of small size analysis is that keeping increasing or decreasing one parameter in a range with fine steps to see the results of the whole system. The Table 9 shows the small changes for M3, M4 and M5 and the width of isolation regions after changing the size of each transistor. In Table 9, it also provides an arithmetic mean and a geometric mean for comparing. Since it minimize the width of isolation region, geometric mean should not be a huge difference. Thus it only focus on the arithmetic mean. Fig.11 is corresponding to the data in Table 9. The simulation for here is to change the size of one transistor every time and provide the data of width of isolation region. Here, the simulation is using the “node-set” method under Inverse Widlar circuit. And the output is the node voltage of node A. The process used is the AMI 0.5μm process. The original size of each transistor, supply voltage and node-setting voltage for each node are given in Table 8.

Table 8. Simulation environment (8)

| | | | |
|---|---|---|---|
| Technology(process) | AMI 0.5μm | M1(W/L/M) | 3μ/3μ/5 |
| Supply voltage | 5V | M2(W/L/M) | 3μ/3μ/5 |
| Output node | A | M3(W/L/M) | 1.5μ/3μ/1 |
| Structure | Inverse Widlar | M4(W/L/M) | 110μ/1.8μ/1 |
| Initial $V_A$ | 4.9V | M5(W/L/M) | 2.4μ/600n/1 |

Table 9. Size percentage change verse isolation region

| | | | Left Bound (˚C) | Right Bound (˚C) | Range (˚C) | Arithmetic Mean (˚C) | Geometric Mean (˚C) |
|---|---|---|---|---|---|---|---|
| M3 | 1.485µ | 1% | 67.5 | 77.4 | 9.9 | 72.45 | 72.28 |
| | 1.47µ | 2% | 65.8 | 80.2 | 14.4 | 73 | 72.64 |
| | 1.425µ | 5% | 62.8 | 86.8 | 24 | 74.8 | 73.83 |
| | 1.35µ | 10% | 57.7 | 97.5 | 39.8 | 77.6 | 75.00 |
| | | | | | | | |
| M4 | 111.1µ | 1% | 70.5 | 73.5 | 3 | 72 | 71.98 |
| | 112.2µ | 2% | 69.9 | 74.2 | 4.3 | 72.05 | 72.02 |
| | 115.5µ | 5% | 68.9 | 75.4 | 6.5 | 72.15 | 72.08 |
| | 121µ | 10% | 67.8 | 77 | 9.2 | 72.4 | 72.25 |
| | | | | | | | |
| M5 | 2.424µ | 1% | 67.9 | 76.8 | 8.9 | 72.35 | 72.21 |
| | 2.448µ | 2% | 66.5 | 79 | 12.5 | 72.75 | 72.48 |
| | 2.52µ | 5% | 64 | 83.9 | 19.9 | 73.95 | 73.28 |
| | 2.64µ | 10% | 61.5 | 90.1 | 28.6 | 75.8 | 74.44 |
| | | | | | | | |
| **Standard** | **0** | **0%** | **71.5** | **72.4** | **0.9** | **71.95** | **71.95** |

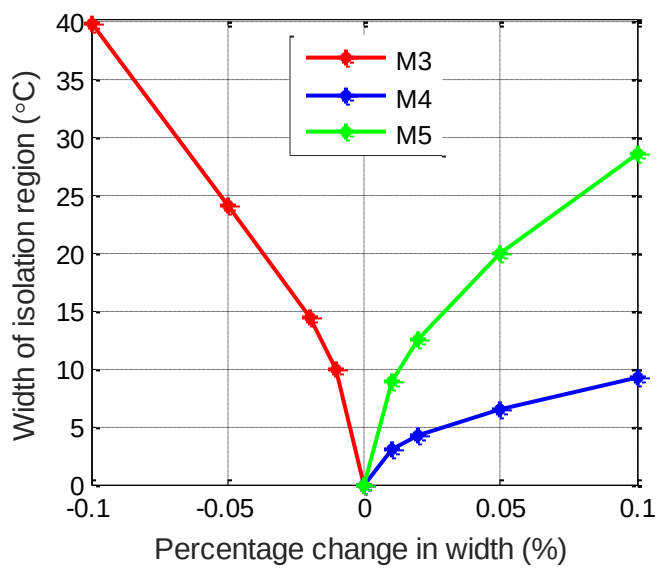



Figure 11. Temperature range with percentage change in transistors size

With the assistance of plot [Fig.11], it can see the curve change smooth and continue, which provides the evidence that the simulation result is correct and the "node-set" method is able to get the correct edge of isolation region. Another clue is that high percent change in width of each transistor will causes the big change in width of isolation region. From the table, it is obvious that the center point (arithmetic mean) of the isolation region are around 72 degree once it minimize the width of Isolation Region. Thus a guess is been made that the center point of isolation region will be fixed once it minimize the width of isolation region in different size combination of each transistor.

To verify the guess, it simulate the circuit with four groups of different combination size and then check the width of isolation region. From Table 10, it is easily to get a result that arithmetic mean is around 72 degree. Also, in Table 11, it simulate the circuit in different corner and get the result that the center point of isolation region is fixed as well.

Table 10. Different size of transistors

| M3 | M4 | M5 | Left Bound(˚C) | Right Bound(˚C) | Range (˚C) | Arithmetic Mean(˚C) | Geometric Mean(˚C) |
|---|---|---|---|---|---|---|---|
| 1.5μ | 42.5μ | 2.7μ | 71.1 | 72.3 | 1.2 | 71.7 | 71.70 |
| 1.5μ | 29.8μ | 2.85μ | 71 | 72.2 | 1.2 | 71.6 | 71.60 |
| 1.5μ | 206.6μ | 2.25μ | 71.6 | 72.6 | 1 | 72.1 | 72.10 |
| 1.653μ | 110μ | 2.7μ | 71.6 | 72.3 | 0.7 | 71.95 | 71.95 |

Table 11. Simulation result of transistors in different corner

| M3 | M4 | M5 | Left Bound (˚C) | Right Bound (˚C) | Range (˚C) | Arithmetic Mean (˚C) | Geometric Mean (˚C) | NMOS | PMOS |
|---|---|---|---|---|---|---|---|---|---|
| 1.5μ | 85.9μ | 2.4μ | 71.5 | 72.1 | 0.6 | 71.8 | 71.80 | fast | slow |
| 1.5μ | 312μ | 2.4μ | 71.6 | 72.5 | 0.9 | 72.05 | 72.05 | slow | slow |
| 1.5μ | 373μ | 2.4μ | 71.6 | 72.8 | 1.2 | 72.2 | 72.20 | slow | fast |
| 1.5μ | 208μ | 2.4μ | 71.7 | 73.1 | 1.4 | 72.4 | 72.40 | fast | fast |

### 4.2 The performance of Isolation Region under IBM 0.13μm Process

In IBM0.13 process, isolation region shows different feature compared to AMI 0.5μm process. Control the isolation region become more convenient and we are able to change either location or width in IBM 0.13μm process. It is a big process since it can only change the width of isolation region in AMI 0.5μm process because of fixed center point. By changing size of different transistors, it is able to find the evidences to show the isolation region is moveable in IBM 0.13μm process. Following are examples show isolation region could be in different location. The simulation of the example is using the "node-set" method under Inverse Widlar circuit. And the output is the node voltage of node A. Each simulation below contains three simulation results with different node-setting voltage. The process used is the IBM 0.13μm process. The supply voltage and node-setting voltage for each node are given in Table 12.

In Table 13, it is showing three examples of isolation region, and they are all in different location but almost same width, which is about 10 $^{o}$C. From the Table 13, it is obvious that they are three different size combinations. The corresponding graph are representing in Fig.12. We can see the isolation region is move from 55.1 $^{o}$C to 95.9 $^{o}$C with almost same width. It prove that the isolation region in IBM process is moveable. Besides the changing the location of isolation region, it also shows the changeable width in Table 14. Two corresponding results are showing in Fig.14, which reveal the controllable width of Isolation Region. From the Fig.14, it shows the width of isolation can be changed from 14.3 $^{o}$C to 42.9 $^{o}$C by different size combination, which provide the evidence of changeable size of isolation region in IBM process.

Table 12. Simulation environment (9)

| | | | |
|---|---|---|---|
| Technology(process) | IBM 0.13 μm | Initial $V_A(1)$ | 1.2V |
| Supply voltage | 1.2V | Initial $V_A(2)$ | 1.08V |
| Output node | A | Initial $V_A(3)$ | 0.7V |
| Structure | Inverse Widlar | | |

Table 13. Different size of transistors verse different location of Isolation Region

| Isolation Region (˚C) | Size of each transistor(W/L/M) | | | | |
|---|---|---|---|---|---|
| | M1 | M2 | M3 | M4 | M5 |
| 55.1~65.3 | 1/0.6/60 | 1.2/1.2/1 | 1.96/0.6/1 | 0.43/0.6/1 | 0.18/4/1 |
| 67.3~81.6 | 1/0.6/60 | 1.2/1.2/1 | 1.98/0.6/1 | 0.48/0.6/1 | 0.21/4/1 |
| 85.7~95.9 | 1/0.6/60 | 1.2/1.2/1 | 2.04/0.6/1 | 0.5/0.6/1 | 0.25/4/1 |

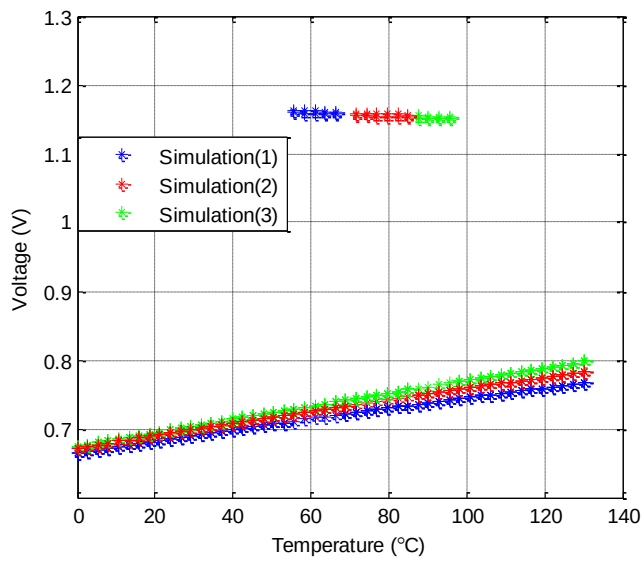
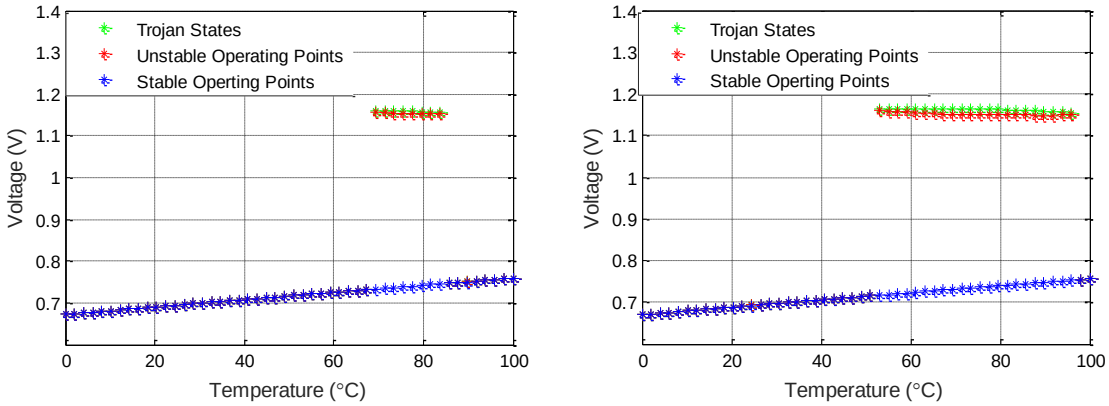



Figure 12. Different location of isolation region

Table 14. Different size of transistors verse different width of Isolation Region

| Isolation Region (˚C) | Size of each transistor (W/L/M) | | | | |
|---|---|---|---|---|---|
| | M1 | M2 | M3 | M4 | M5 |
| 69.3~83.6 | 1/0.6/60 | 1.2/1.2/1 | 1.98/0.6/1 | 0.48/0.6/1 | 0.21/4/1 |
| 53.0~95.9 | 1/0.6/60 | 1.2/1.2/1 | 1.98/0.6/1 | 0.50/0.6/1 | 0.21/4/1 |




(a) (b)

Figure 13. Different Width of Isolation Region

### 4.3. Isolation Region in Wilson circuit

Many temperature sensor and reference generator circuits use positive feedback loops to reduce output sensitivity to the power supply voltage and these circuits are vulnerable to the multiple equilibrium point problem. Start-up circuits are invariably used to keep these circuits operating at the desired equilibrium points.

Since both Wilson circuit and Inverse Widlar have one positive feedback loop, it raise a doubt if there is also an isolation region existing in Wilson circuit. Depending on previous experience, isolation region only happens in condition that the size for each transistor is well designed and it happens in a very small subset of design space. Too small size or too large size will kill the isolation region even hysteresis window. Because Wilson circuit is different structure comparing to Inverse Widlar, the isolation region cannot be found until it use a transitive circuit to get a fluent transition.

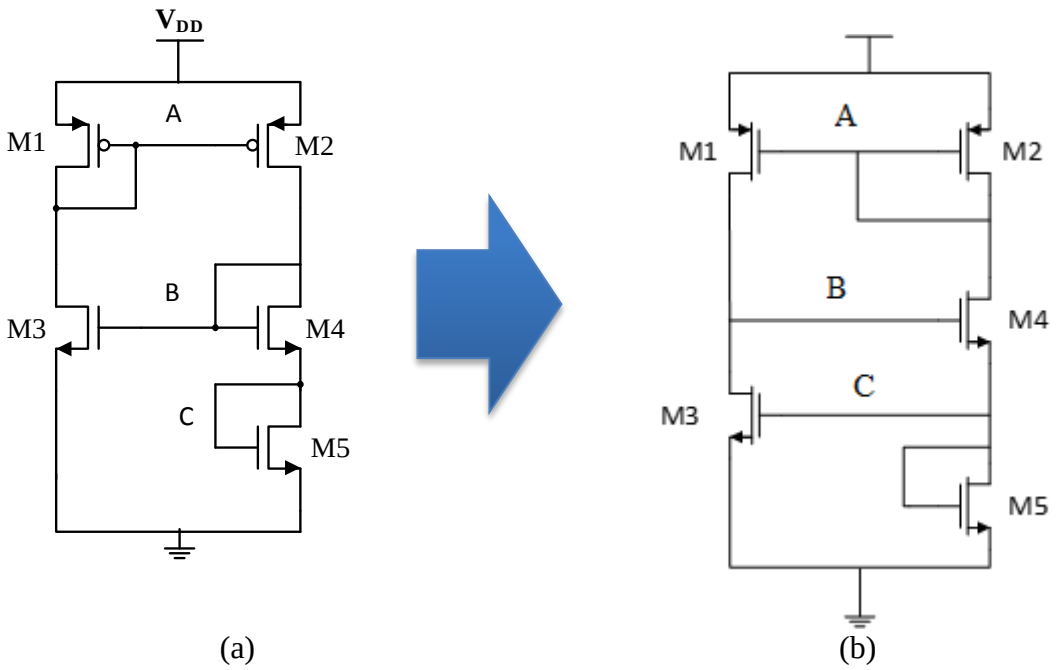



Figure 14. (a) Inverse Widlar circuit (b) Wilson circuit

In Fig.14, it shows the circuit which need to be done transition. Left hand side is Inverse Widlar and right hand side is Wilson circuit. They all share five transistor and current mirror in the top. With adding some resistor, it utilize a transition circuit in Fig.15. The circuit has six transistors with two diode-connections in the bottom and a current mirror in the top. If making the resistor infinite, it will cut down the connection between gate of M3 and gate of M4, and also short the M5. Now it is showing like a Wilson circuit. Once the resistor changes to zero, gate of M3, M4 will be connect to each other and M6 will be shorted. The circuit is showing the characteristic of Inverse Widlar circuit. By using this circuit, it is slightly changing the resistor value from zero to infinite with changing the size of each transistor to keep the existing of Isolation Region. Finally, isolation region is successfully made in Wilson circuit. Fig.16 shows the Isolation Region in Wilson circuit. Here, the figure contains three simulation results and they are using the “node-set” method by using different node-setting voltage under Wilson circuit. And the output is the node voltage of node A. The process used is the AMI 0.5 μm process. The size of each transistor, supply

voltage and different node-setting voltages for node A are given in Table 15. From the Fig16, we can see the isolation region is existing in Wilson circuit between 45.71 $^{o}$C and 142.9 $^{o}$C.

Table 15. Simulation environment (10)

| | | | | | |
|---|---|---|---|---|---|
| Technology(process) | AMI 0.5 µm | M1(W/L/M) | 60 µ/1.5 µ/10 | Green | 4.9V |
| Supply voltage | 5V | M2(W/L/M) | 3 µ/3 µ/4 | Red | 4.5V |
| Output node | A | M3(W/L/M) | 2.55 µ/1.8 µ/1 | Blue | 3.2V |
| Structure | Wilson | M4(W/L/M) | 1.5 µ/3 µ/1 | | |
| | | M5(W/L/M) | 3 µ/600n/1 | | |

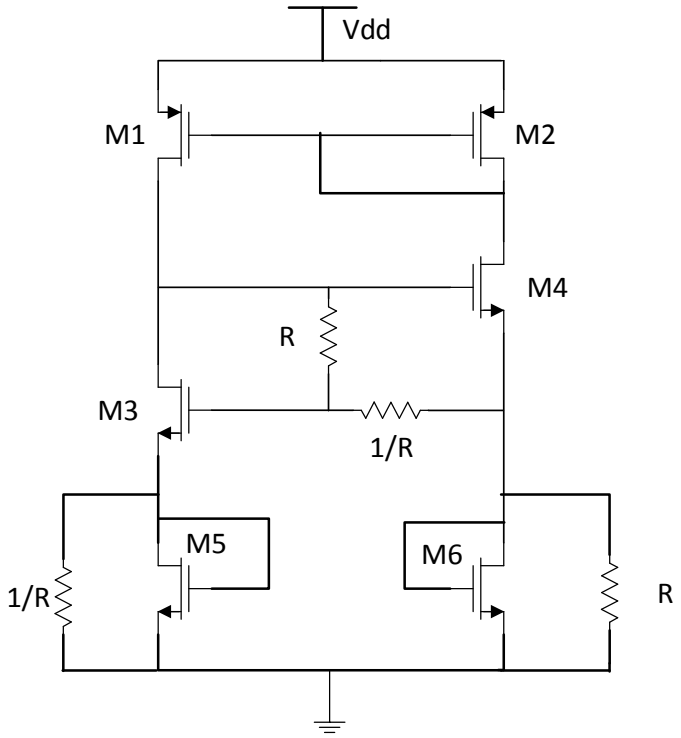



Figure 15. Transition circuit

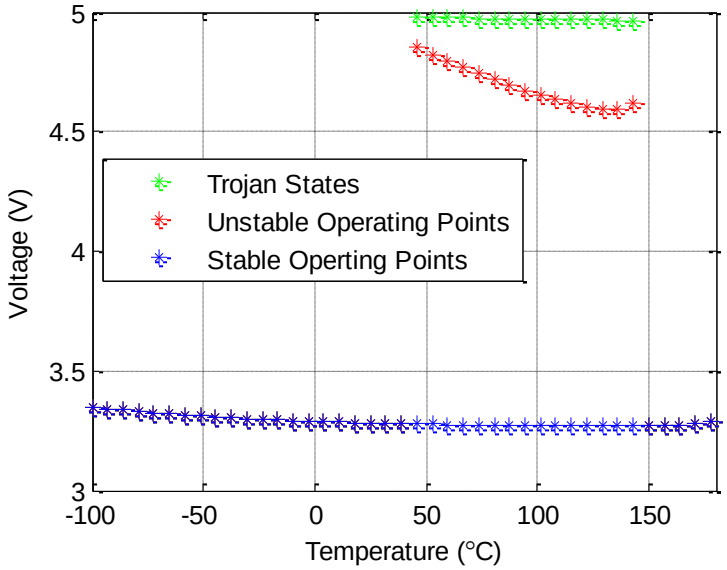



Figure 16. Isolation Region in Wilson circuit

# CHAPTER V

# PROTOTYPE CIRCUIT FOR ISOLATION REGION

This chapter will present a prototype circuit for isolation region and it could be used as a Hardware Trojan. It will describe the schematic of the circuit, layout, and control methods for this Hardware Trojan vulnerability. For this prototype circuit, it is based on inverse Widlar structure and under AMI 0.5μm process. Highly hidden and controllable are two key features of this hardware Trojan vulnerability. Since it is able to control the width of isolation region, isolation region is easy to be hidden in the circuit and inexperience designer has high possibility to miss the isolation region due to ignore putting start-up circuit. The target for this part is to reveal a new method of creating hardware Trojan and recognize designers to take care of this vulnerability when they are doing circuit designing.

## 5.1 The schematic of prototype circuit

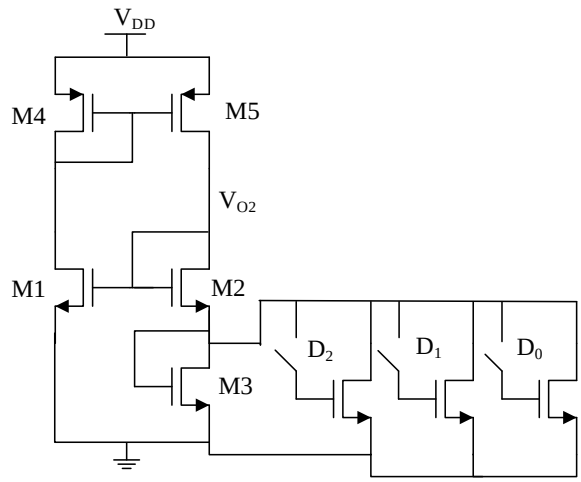



Figure 17. Schematic of hardware Trojan vulnerability

Here is an Inverse Widlar circuit [Fig.17] with three binary controls so that it can change the size of one transistor (here is M3). The reason why choosing the Inverse Widlar is that Inverse Widlar circuit has simple structure and easy to control. All simulation result are using AMI 0.5μm process and layout is also under this process. Based on the simulation, it only needs to change one transistor to change the width of isolation region. In addition, it can also make isolation region disappear or appear of hysteresis window in the circuit.

Table 16. Transistor size (1)

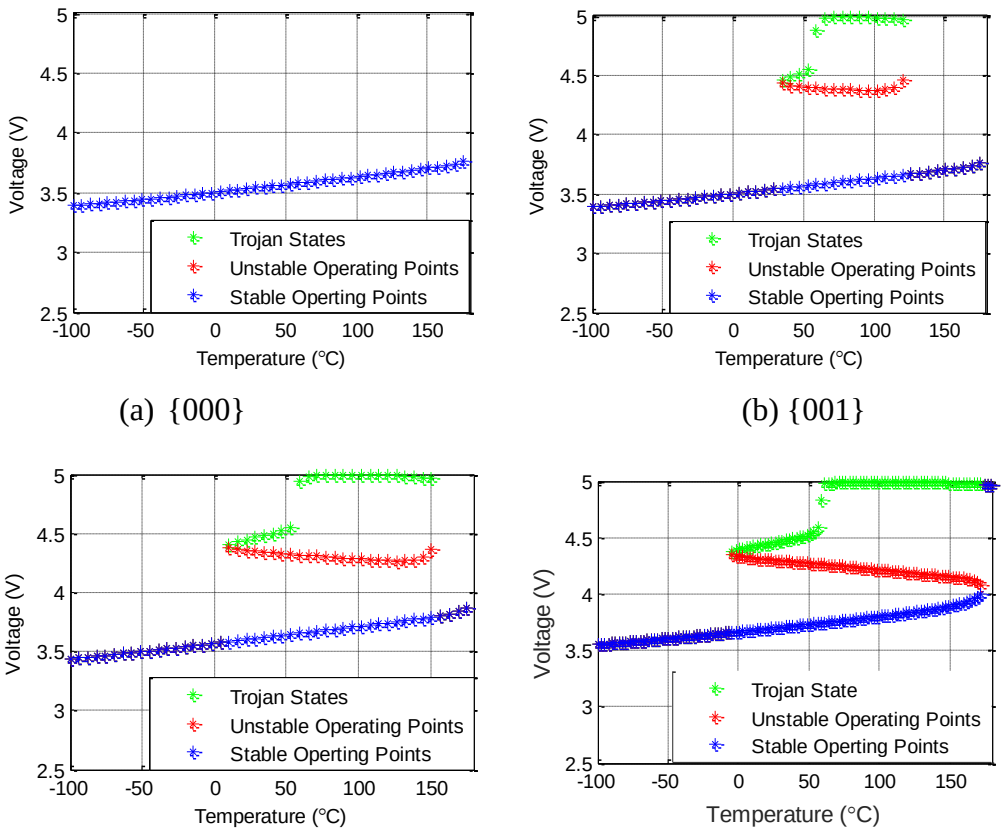
| Transistor | M1 | M2 | M3 | M4 | M5 |
|---|---|---|---|---|---|
| Size(W/L/M) | 1.5μ/3μ/1 | 4.95μ/1.8μ/1 | 4.5μ/600n/1 | 3μ/3μ/5 | 3μ/3μ/5 |

Table 17. Transistor size (2)

| Transistor | D0 | D1 | D2 |
|---|---|---|---|
| Size | $(\frac{5\mu}{600n})_{m=2}$ | $(\frac{5\mu}{600n})_{m=4}$ | $(\frac{5\mu}{600n})_{m=8}$ |

## 5.2 The performance of Hardware Trojan

Based on the simulation result, the circuit will have only one operation in temperature range (-100 ℃ to 200 ℃). When connecting the extra NMOS to the M3 (which means the width of M3 is increasing), it will shows the isolation region [Fig.18]. Keep increasing the circuit will shows the hysteresis windows. The following figures describe one of the conditions that isolation region appears in the simulation results. Through the figures below, we can see the appearance of isolation region and hysteresis window.




(a) {000} (b) {001}

(c) {100} (d) {111}

Figure 18. Simulation result for isolation region

### 5.3 Layout of the circuit

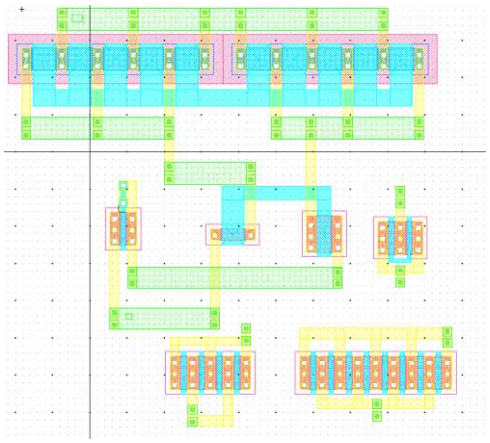


Figure 19. Core of the hardware Trojan

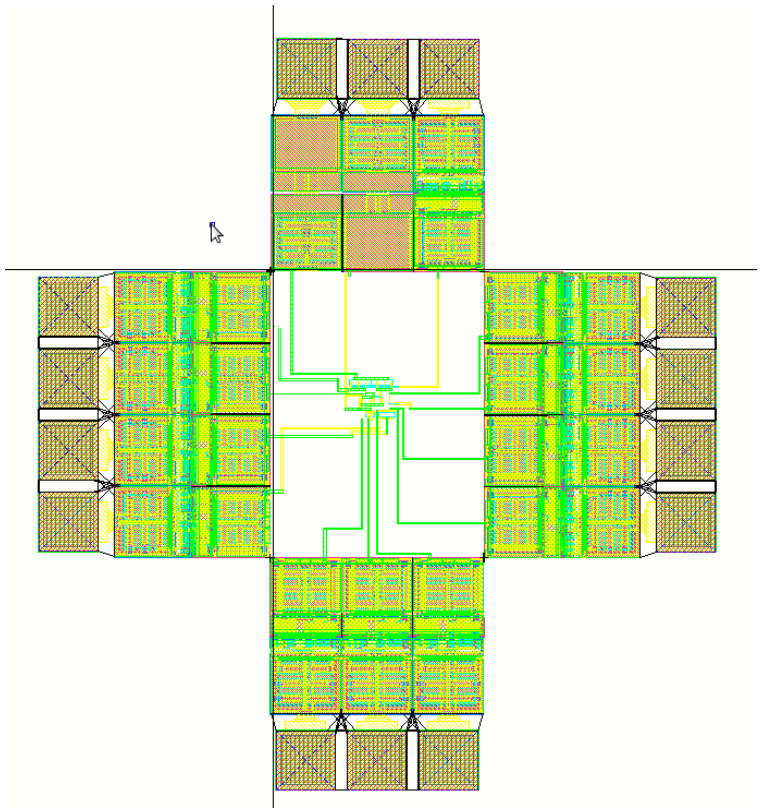


Figure 20. Top level of hardware Trojan vulnerability

The total are of the chip is 880 * 973 = 856240 $um^2$

# CHAPTER VI

# CONCLUSION

Two methods that can be used to identify the presence of multiple stable equilibrium points with a standard circuit simulator in some analog circuits that have a single positive feedback loop were discussed. One is based upon a bidirectional temperature sweep from which multiple stable equilibrium points can often be identified if a hysteresis loop appears. The other is based upon using the node-set feature to start a simulation at a given temperature in the region of attraction of an unknown equilibrium point. Both methods attempt to exploit the property that if more than one stable equilibrium points exists, then the number of equilibrium points in the circuit is often temperature dependent.

The concept of an isolation region in the temperature characteristics of a circuit was discussed. It was shown that the designer can control the location and the size of the isolation region in the inverse Widlar structure. A continuation method was used to show that an isolation region can also occur in the popular Wilson bias generator. Detection of the presence of an isolation region with standard circuit simulation and verification tools can be very challenging, particularly if the size of the isolation region is small. This property creates a vulnerability for adversarial engineers to exploit the isolation region by using it to embed analog hardware Trojans that are extremely difficult to detect. These analog hardware Trojans are particularly insidious because they require no additional components, leave no signatures in either circuit timing or the power supply bus prior to triggering, and are often completely transparent even if a complete and accurate circuit schematic is available. Analog hardware Trojans embedded in an isolation region present a severe threat to the security of financial, medical, transportation, and military systems.

## REFERENCES

[1] Wikipedia, http://en.wikipedia.org/wiki/Hardware_Trojan.

[2] R. Geiger, "Senior Design Project Proposal", Electrical and Computer Engineering Department, Iowa State University, Fall 2014.

[3] Bhunia, Swarup, et al. "Hardware Trojan Attacks: Threat Analysis and Countermeasures." Proceedings of the IEEE 102.8 (2014): 1229-1247.

[4] Wikipedia, "https://en.wikipedia.org/wiki/Integrated_circuit_design".

[5] M. Tehranipoor, F. Koushanfar. "A Survey of Hardware Trojan Taxonomy and Detection," *IEEE Des. Test.Comput.*, vol. 27, no. 1, pp.10-25, Feb. 2010.

[6] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, B. Sunar. "Trojan Detection Using IC Fingerprinting," in *Proc. IEEE Symp. Security Privacy*, pp.296-310, 2007.

[7] J. Li, J. Lach. "At-Speed Delay Characterization for IC Authentication and Trojan Horse Detection," in *Proc.Hardware-Oriented Security and Trust Conference (HOST)*, pp.8-14, 2008.

[8] S. Jha and S. K. Jha, "Randomization Based Probabilistic Approach to Detect Trojan Circuits," " in *Proc. 11th IEEE High Assur. Syst. Eng. Symp.*, pp.117–124, 2008.

[9] M. Banga and M. Hsiao, "A region based approach for the identification of hardware Trojans," in *Proc. Hardware-Oriented Security and Trust Conference (HOST)*, pp.40–47, 2008.

[10] G. E. Suh, D. Deng, and A. Chan, "Hardware authentication leveraging performance limits in detailed simulations and emulations," in *Proceedings of the 46th Annual Design Automation Conference (ACM)*, pp.682-687, 2009.

[11] D. McIntyre, F. Wolff, C. Papachristou, and S. Bhunia, "Dynamic evaluation of hardware trust," in *Proc. Hardware-Oriented Security and Trust Conference (HOST)*, pp.108-111, 2009.

[12] Y. Wang, D. Chen, and R.L. Geiger, "Practical Methods for Verifying Removal of Trojan Stable Operating Points", *IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 2658-2661, May 2013.

[13] R.J. Widlar, "Some circuit design techniques for linear integrated circuits", *Circuit Theory*, no. 4 pp. 586-590. 1965.

[14] G.R. Wilson, "A Monolithic Junction FET npn Operational Amplifier", *IEEE Journal of Solid State Circuit*, SC-3, pp. 341-348, Dec. 1968.

[15] H. Banba, H. Shiga, A. Umezawa, T. Miyaba, T. Atsumi, K. Sakui, “A CMOS bandgap reference circuit with sub-1-V operation”, *IEEE Journal of Solid State Circuits*, SC-5, pp. 670-674, 1999.

[16] K.E. Kujik, “A precision reference voltage source”, *IEEE Journal of Solid State Circuit*, SC-3, pp. 222-226, 1973.

[17] A.J. Annema, B. Nauta, R. Van Langevelde, and H. Tuinhout, “Analog circuit in ultra-deep-submicron CMOS”, *IEEE Journal of Solid State Circuits*, SC-1, pp. 132-143, 2005.

[18] D.F. Mietus, “Reference voltage circuit having a substantially zero temperature coefficient”, U.S. Patent No.5,666,046, Sep. 1997.

[19] T. Nishi and L. O. Chua, "Topological criteria for nonlinear resistive circuits containing controlled sources to have unique solution," *IEEE Trans. Circuits Syst.*, vol. 31, no. 8, pp. 722-741, 1984.

[20] L. O. Chua and R. L. P. Ying, "Finding all solutions of piecewise-linear circuits", *Int. J. Circuit Theory Appications.*, vol. 10, pp.201 -229, 1982.

[21] K. Yamamura and T. Ohshima, "Finding all solutions of piecewise-linear resistive circuits using linear programming,*" IEEE Trans. Circuits Syst.-I*, vol. 45, no. 4, pp.434-445, Apr 1998.

[22] L. B. Goldgeisser and M. M. Green, "A method for automatically finding multiple operating points in nonlinear circuits," *IEEE Trans.Circuits Syst. I, Reg. Papers*, vol. 52, no. 4, pp. 776-784, Apr. 2005.

[23] Y. Li, and D. Chen, “Efficient analog verification against Trojan states using divide and contraction method”, *IEEE International Symposium on Circuit and System (ISCAS)*, pp. 281-284, 2014

[24] M. H. Zaki, I. M. Mitchell, and M. R. Greenstreet, “DC operating point analysis - a formal approach,” in *Proceedings of Formal Verification of Analog Circuits (FAC),* 2009.

[25] S. Tiwary, A. Gupta, J. Phillips, C. Pinello, R. Zlatanovici, "First Steps Towards SAT-based Formal Analog Verification," in *Computer-Aided Design-Digest of Technical Papers (ICCAD)*, pp.1-8, Nov. 2009.

[26] L. Yin, Y. Deng and P. Li, “Simulation-Assisted Formal Verification of Nonlinear Mixed-Signal Circuits with Bayesian Inference Guidance” *Computer-Aided Design of Integrated Circuits and Systems*, IEEE Transactions on 32, no. 7, pp.977-990, Jul. 2013

[27] Q. Wang, R.L. Geiger, and D. Chen. "Challenges and opportunities for determining presence of multiple equilibrium points with circuit simulators." *IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 406-409, 2014.

[28] Q. Wang and R.L. Geiger, “Temperature signatures for performance assessment of circuit with undesired equilibrium states”, Electronic Letters, (under review).