2018

Analog hardware security and hardware authentication

Qianqian Wang
Iowa State University

Analog hardware security and hardware authentication

by

Qianqian Wang

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Computer Engineering

Program of Study Committee:
Randall Geiger, Major Professor
Degang Chen
Chris Chu
Meng Lu
Yong Guan

The student author, whose presentation of the scholarship herein was approved by the program of study committee, is solely responsible for the content of this dissertation. The Graduate College will ensure this dissertation is globally accessible and will not permit alterations after a degree is conferred.

Iowa State University

Ames, Iowa

2018

DEDICATION

To my husband and my parents

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

NOMENCLATURE

CMOS	Complementary metal-oxide-semiconductor
VLSI	Very large scale Integration
IC	Integrated Circuit
IP	Intellectual Property
V_{TH}	Threshold voltage
PVT	Process/Voltage/Temperature
PAAST	Power/Architecture/Area/Signature Transparent
Chip	Alternative term for an integrated circuit
COTS	Commercial Off The Shelf integrated circuits
PUF	Physically Unclonable Function

ACKNOWLEDGMENTS

I would like to thank my advisor and committee chair Dr. Geiger for his dedication, guidance, and patience on my work. The joy he has for research and work will always motivate me. I would also like to thank my committee members, Dr. Chen, Dr. Chu, Dr. Lu, Dr. Guan, and Dr. Duwe for their guidance and support throughout the course of this research.

Secondly, I would also like to thank my friends, colleagues, the department faculty and staff for making my time at Iowa State University a wonderful experience. I want to also offer my appreciation to those who were willing to participate in my study and research, without whom, this thesis would not have been possible.

In addition, I would like to thank my family members, my father Lixin Wang, my mother Xiuju Chen, my sister Qianlan Wang. Nobody has been more important to me than them, whose love and encouragement are always with me. Most importantly, I would like to thank my husband Shixin Tian for his love, respect, patience, and continuous support.

This work was supported, in part, by NSF through award 1509538 and by SRC through award numbers 1705122 and 639581.

ABSTRACT

Hardware security and hardware authentication have become more and more important concerns in the manufacture of trusted integrated circuits. In this dissertation, a detailed study of hardware Trojans in analog circuits characterized by the presence of extra operating points or modes is presented. In a related study, a counterfeit countermeasure method based upon Physically Unclonable Function (PUF) authentication circuits is proposed for addressing the growing proliferation of counterfeit integrated circuits in the supply chain.

Most concerns about hardware Trojans in semiconductor devices are based upon an implicit assumption that attackers will focus on embedding Trojans in digital hardware by making malicious modifications to the Boolean operation of a circuit. In stark contrast, hardware Trojans can be easily embedded in some of the most basic analog circuits. In this work, a particularly insidious class of analog hardware Trojans that require no architectural modifications, no area or power overhead, and prior to triggering, that leave no signatures in any power domains or delay paths is introduced. The Power/Architecture/Area/Signature Transparent (PAAST) characteristics help the Trojan "hide" and make them very difficult to detect with existing hardware Trojan detection methods. Cleverly hidden PAAST Trojans are nearly impossible to detect with the best simulation and verification tools, even if a full and accurate disclosure of the circuit schematic and layout is available. Aside from the work of the author of this dissertation and her classmates, the literature is void of discussions of PAAST analog hardware Trojans. In this work, examples of circuits showing the existence of PAAST analog hardware Trojans are given, the PAAST characteristics of these types of hardware

Trojans are discussed, and heuristic detection methods that can help to detect these analog hardware Trojans are proposed.

Another major and growing problem in the modern IC supply chain is the proliferation of counterfeit chips that are often characterized by different or inferior performance characteristics and reduced reliability when compared with authentic parts. A counterfeit countermeasure method is proposed that should lower the entry barrier for major suppliers of commercial off the shelf (COTS) parts to offer authenticated components to the military and other customers that have high component reliability requirements. The countermeasure is based upon a PUF authentication circuit that requires no area, pin, or power overhead, and causes no degradation of performance of existing and future COTS components.

CHAPTER 1. INTRODUCTION

1.1 Background and Motivation

Security, dependability, and trust of electronic systems are essential in a world that is so dependent upon the uninterrupted world-wide operation of a globe-scale electronic communication and information network. Over the past several decades there have been numerous attempts by dubious individuals to compromise various components in this monstrous network. These attempts include malicious software attacks, often termed viruses, which result in denial of services, in stealing information, in stealing money, in destroying or altering valuable data, etc. The computer programs that harbor these viruses are often termed software Trojans. Software Trojan attacks are an ongoing problem with multiple attack threads running at different locations around the world every day. High levels of resources are continually invested to counter these attacks and constrain the impact of these attacks to a level that does not dramatically compromise the operation of the system. Though these software attacks are continuously ongoing and though they are much more than an annoyance, society is accustomed to functioning with these attacks and the ongoing efforts to minimize the impact of software Trojans actually strengthen the overall reliability and integrity of our cyber infrastructure. Software security will remain an area of ongoing research activity for the foreseeable future.

The adversarial modification of an integrated circuit to intentionally alter the behavior of the circuit in some devious way introduces what is termed a “Hardware Trojan” into the IC. Electronic systems are also vulnerable to hardware breaches. But unlike software breaches which regularly occur and routinely mitigated by making software changes, hardware breaches can render the associated hardware permanently compromised. If a

hardware Trojan were to be embedded into hardware that is widely distributed and if that hardware Trojan were to remain dormant for an extended period of time and then triggered, all hardware that contained that Trojan would be compromised. Imagine, for example, what would happen if a hardware Trojan were embedded in a key hardware component that was common to all Apple iPhones that were sold over a period of two years and that it was designed to lay dormant for a two-year period. That hardware Trojan would affect close to 500 million users when triggered and could require a hardware modification to mitigate the Trojan. The impact such a Trojan could have on society would be devastating.

In contrast to software Trojans that occur regularly, there is no documented evidence of a single hardware Trojan that has been successfully embedded into any integrated circuit that is in production today. But numerous research works show the vulnerability that exists in the hardware fabric of todays' electronic systems to the introduction of hardware Trojans. In contrast to the routinely encountered software Trojans which usually have a modest but manageable negative impact on computer system security, hardware Trojans could have a much more devastating impact on cyber security. For these reasons, hardware security is of growing concern.

Maintaining a high level of hardware security is becoming more and more challenging nowadays due to the fact that there are multiple places in the normal production flow of an integrated circuit where hardware breaches can be inserted. Due to globalization of the IC industry, the physical locations where the breaches can be inserted are distributed throughout the globe thereby making it even more difficult to maintain a high level of hardware security.

Various stages in the production flow of an IC where hardware Trojans can be inserted include the design, layout, fabrication, and testing stages. Outsourcing of parts of the design, of the fabrication, and the growing use of third-party IP increase hardware security risks. More research is needed on understanding the vulnerability to hardware Trojans and on strategies to mitigate these vulnerabilities.

The motivation for an individual or individuals to insert hardware Trojans into one or more ICs may be much different than the motivation to insert software Trojans into the cyber network. Regardless of the motivation, inserting a Trojan is evil, illegal and disruptive. Hackers may view the insertion of software Trojans as a challenge and a distorted way to demonstrate cleverness to their peers. Others may insert software Trojans for financial gain or possibly for political gains. In contrast, it is highly unlikely that hackers will have either the knowledge or access needed to target insertion of hardware Trojans. The profile of the most likely hardware hacker that would be in a position to insert a hardware Trojan is an experienced and trusted design or process engineer with a high-level of access to the design and/or production process. Though it is possible that the person could be a disgruntled or deranged employee, it would more likely be a person that was highly trained and strategically placed by an adversary with a long-term goal of being in a position to insert the hardware Trojan. And unlike perpetuators that insert software Trojans that may be difficult to identify, it is highly likely that the identity of those responsible for inserting a hardware Trojan would be quickly determined once the hardware Trojan is activated. For these reasons, a perpetuator that would be in a position to insert a hardware Trojan will be referred to as an adversary. A trusted individual in a company that actually works to sabotage the output is often termed a "mole".

Most concerns about hardware Trojans in semiconductor devices are based upon an implicit assumption that adversaries will target embedding hardware Trojans in the digital hardware of an IC and the Trojan will be a malicious modification of the Boolean operation of the circuit. Invariably these hardware Trojans require a modification or generally an addition of some components into the circuit and during normal operation of the circuit, the presence of these Trojans introduce signatures in power supply domains, signatures or timing changes in signal paths of the circuit, and/or delays of signals propagating in the circuit. Efforts to thwart hardware Trojans are often associated with identifying architectural modifications, trigger mechanisms, the presence of payloads, or through side channel analysis by observing signatures in the power bus or delay paths that differ from what is expected in a Trojan-free circuit [1]-[5]. Correspondingly, there are few reported concerns in the trust and security communities about the vulnerability of analog circuits to the malicious insertion of hardware Trojans. Unfortunately, analog hardware Trojans can be easily inserted in some of the most basic analog circuits [6],[7] , they can be easily triggered, they can carry devastating payloads, and they can be extremely difficult to detect.

Although analog hardware Trojans could be introduced by incorporating additional analog circuitry or altering a design, existing methods of hardware Trojan detection can be adapted to help thwart such Trojan insertions. However, existing methods are not effective at detecting a Trojan that is embedded as an extra state or operating mode that may be inherent in what may appear to be a well-designed circuit. Hardware Trojans served by the extra undesired state or operating mode are power/ area/ architecture/signature transparent. Prior to triggering such a circuit to operate in the undesired state or mode, which will be termed the Trojan state or the Trojan mode, the circuit will not demonstrate any abnormal

signatures. Thus, all existing hardware Trojan detection methods which depend upon identifying alterations in the circuit structure or abnormal signatures in electrical characteristics during normal operation will fail to detect this kind of Trojan.

In this dissertation, a type of analog hardware Trojans that are embedded as extra operating states or modes in an analog circuit will be discussed. These Trojans require no additional power, no architectural modifications, no area changes, and, prior to triggering, leave no signatures in the power bus or delay paths. These Trojans will be descriptively termed PAAST Trojans because they are Power/Area/Architecture and Signature Transparent. And, of the moles that design the PAAST Trojans make them stealthy, these Trojans will also invariably escape detection through the design and verification steps with the best existing simulation and verification tools even if full and accurate disclosure of the entire circuit schematic and layout is available.

Another major and growing problem in the modern IC supply chain is the proliferation of counterfeit chips [8]. Driven by financial incentives, unscrupulous enterprises insert these chips into the supply chain in a variety of ways, such as recycling used chips from disassembled boards, remarking inferior components, manufacturing unauthorized wafers, or even designing chips with similar but meaningfully different characteristics. There are conflicting estimates of the size of the counterfeit IC market. This is not surprising since considerable effort is often required to determine if an IC has been counterfeited. One report [9] out of ST Microelectronics in Europe suggested that in 2011 it was around 1% of semiconductor sales and another report [10][11] from the International Trade Administration of the US Department of Commerce report it around 5% of semiconductor sales in the same

year. But there is no disagreement that the counterfeit IC market is growing rapidly and that it is a large market.

Chip counterfeiting has not yet reached the level needed to provide the impetus for major chip manufacturers to address the problem because the revenue loss as a percent of sales is still relatively low and because producers of high volume consumer electronic equipment do not demand high reliability components from the semiconductor supply chain. However, counterfeit components that perform differently or that are not reliable can cause catastrophic problems when they find their way into military systems, transportation systems, precision healthcare, or other applications where a high level of reliability is essential. It is well known that Physical Unclonable Functions (PUFs) can be used for providing low-cost IC authentication. The PUFs add a unique identity (e.g. fingerprint) to each integrated circuit. Circuit-based PUFs rely on the inherent manufacturing variability of the physical characteristics of silicon to generate the unique fingerprints for each IC [12]-[15]. The major semiconductor manufacturers of COTS parts are, however, reluctant to add authentication circuits to their integrated circuits primarily due to concerns about increased die area, increased pin count, and concerns about potential interference with the intended operation of a circuit [16]. If the entry barrier for including authentication capabilities can be sufficiently lowered, including authentication as a standard part of the COTS production flow can add financial incentives for manufacturers to address the counterfeit IC problem. Demanding customers, such as the transportation industry, financial organizations, and the military would then have access to parts with a very low counterfeit rate.

In this dissertation, a detailed study of PAAST analog hardware Trojans is presented. Prototype circuits that are designed to harbor PAAST Trojans both as undesired static

operating states and undesired dynamic modes of operation are presented. Characteristics of the PAAST Trojans are discussed along with stealthy triggering mechanism. Methods for detecting the presence of some types of PAAST analog Trojans are introduced. A PUF-based under-circuit designed without any extra pins or interaction with the COTS IC is proposed for IC authentication.

1.2 Dissertation Organization

A discussion about the existence of undesired static operating points and undesired dynamic modes of operation in the circuit along with a discussion of how they serve as hardware Trojans appears in Chapter 2. The vulnerability of circuits to the presence of multiple operating points or modes along with general characteristic of PAAST circuits is discussed in Chapter 2. Several basic circuits with embedded PAAST Trojans that can serve as benchmarks and example circuits with three different temperature signature characteristics are introduced in Chapter 2. Circuits with multiple stationary dynamic modes of operation where the undesired mode of operation are deviations in amplitude, frequency, and phase are also discussed.

In Chapter 3, detection methods for verifying the existence of PAAST Trojans are proposed. Included is a temperature sweeping method that is compatible with basic simulation tools. A method that can be used to identify the presence or absence of stationary dynamic Trojan operating modes based upon the phase-plane characteristics of dynamic circuits is presented in Chapter 3.

Side channel trigger mechanisms that serve as PAAST triggers for dynamic circuits are discussed in Chapter 4 along with measurement results for discrete-component implementations of these circuits.

The implementation of a PUF-based IC authentication approach appears in Chapter 5. It is based upon an under-circuit that generates a unique key for each IC.

Chapter 6 comprises a conclusion of this work.

CHAPTER 2. PAAST HARDWARE TROJANS IN ANALOG CIRCUITS

The PAAST Trojans can be easily embedded in many commonly used analog circuits such as voltage/current reference generators, temperature sensors, phase-locked loops, oscillators and clock generators, data converters, amplifiers, power management circuits, and a wide variety of filters. And, because of the area, power, and signature transparency, in addition to escaping detection during design and verification, almost all existing methods of hardware Trojan detection will fail to detect these Trojans. Since the PAAST Trojans can be easily inserted into some of the most basic analog blocks and since they are extremely difficult to detect, the analog circuitry must be viewed as fertile ground for the adversarial insertion of insidious hardware Trojans.

The hardware Trojan discussed in this dissertation is characterized by the presence of extra equilibrium states or extra stationary dynamic operating modes. The extra states or extra modes are undesired and if operation is forced into the undesired state or mode, the Trojan is said to be triggered. Vulnerability of a circuit to harboring these Trojans is based upon an open problem in the mathematics and computer science communities. Qualitatively, this problem can be summarized by the observation that there are no known methods for obtaining all solutions of a finite set of constrained nonlinear differential equations in finite time [17]-[21]. And, even with the small set of equations that characterize some simple analog circuits with only a few devices, such as those commonly used in voltage/current reference generators, temperature sensors, … , there are no known methods for even determining if all the existing solutions for these circuits in an efficient time. But, just because there are no known methods for determining if a nonlinear circuit has more than one

solution, likely most useful nonlinear circuits have only a single solution and thus will not harbor a PAAST Trojan.

The open problem that provides cover for PAAST Trojans is based on the possible presence of more than one solution to a set of nonlinear equations where an undesired solution corresponds to a Trojan state. Invariably the set of nonlinear static circuit equations come from nonlinear circuits that incorporate energy storage elements and thus the nonlinear equations are also dependent upon time. The solutions of a static nonlinear circuit can be separated into two mutually exclusive groups. One group corresponds to those static solutions (also termed "dc equilibrium points" or simply "equilibrium points") that correspond to a stationary solution of the time-dependent circuit and the other group corresponds to a non-stationary solution of the time-dependent circuit. The stationary solutions are termed "stable equilibria" by some authors. Those dc equilibrium points that are not stationary are termed "quasi-stable" operating points. PAAST Trojans in the static operation of a circuit are associated with the presence of one or more undesired stationary solutions. DC equilibrium points that are quasi-stable do not harbor Trojans since the circuit will always drift away from solutions that are not stable equilibria. In the control systems community, relationships between stability, metastability, and instability and the corresponding static solutions of a set of nonlinear equations are often discussed but this formalization is not germane to the results presented in this dissertation.

Some specific nonlinear circuit structures are known for supporting more than one stationary solution. One of the most commonly used circuits in all of electronics has three dc equilibrium points, two of which are stationary equilibrium points with the third solution being a quasi-stable equilibrium point. That circuit is the four-transistor two-inverter latch.

In the case of the two-inverter latch, which will be discussed in more detail in the following section, the two stationary equilibrium points are actually both desired operating points with one representing the Boolean "0" value and the other representing the Boolean "1" value. By adding a small amount of control circuitry, the user can force operation into either of the two stationary states. It can be observed that for useful implementations, the circuit structure of the basic two-inverter latch incorporates a positive feedback loop in the small-signal linear circuit schematic when both inverters are operating in the vicinity of the quasi-stable operating point. This simple example shows that the existence of multiple stationary equilibrium points for a nonlinear circuit is not inherently bad and, to the contrary, can be very useful. But if a circuit has an undesired stationary equilibrium point and if the presence of that undesired stationary equilibrium point is difficult to recognize and causes undesired behavior of the circuit, then the undesired stationary solution can be viewed as a Trojan state or Trojan mode of operation.

Numerous authors have expressed interest in developing strategies for determining whether a circuit has more than one stationary solution. Willson [62] showed that for circuits comprised of bipolar transistors, resistors, and independent sources, a necessary condition for the existence of bistable solutions is the presence of at least two transistors along with a specific type of feedback structure in the circuit. In subsequent work [22], he showed that "all circuits constructed by interconnecting, in an arbitrary manner, two bipolar transistors and an arbitrary number of resistors and independent sources, posses, at most three dc equilibrium points". Goldgeisser and Green [30] observed that at least some of the results for circuits with bipolar transistors do not extend to circuits with MOS transistors by providing an example of a circuit with two MOS transistors that has five equilibrium points.

Inoue and colleagues [23] stated "…it is known that, when the circuit has positive feedback loops, it may have multiple solutions" though it is not clear that they correctly interpreted the referenced literature. But what these and other authors have observed is that some type of feedback is present in transistor circuits that have more than one equilibrium point. The author of this work is not aware of the existence of any transistor circuits without a feedback path that have more than one equilibrium point.

But making statements about the relationship between the presence of more than one equilibrium point in transistor circuits and the presence of an associated feedback path is complicated by what appears to be the lack of a consensus on how feedback itself is defined. The concept of feedback has been used for centuries in the design of mechanical systems and it has been formally used for over 100 years in the electrical and electronic circuits' field. In the electronics field, invariably the feedback in a circuit is discussed in the context of a block diagram or a graphical representation of a circuit and both representations suppress information about the circuit. Further, multiple block diagrams and multiple graphical representations are common for a given circuit and consequently multiple feedback representations of a circuit are possible. Even after a block diagram or a graphical representation is obtained, there are different ways that a feedback loop can be defined. Feedback is often characterized as being "positive" or "negative" and even these terms are not uniquely defined for a given circuit. As such, making a general rigorous statement relating the presence or absence of multiple equilibrium points in a circuit to a feedback structure is challenging and beyond the scope of this work. Without formally defining feedback, positive feedback, or negative feedback, conventional wisdom relating to the

relationship between the presence or absence of multiple stationary equilibrium points in a transistor circuit can be summarized by the statement

"A necessary but not sufficient requirement for the existence of more than one stationary equilibrium points in a transistor circuit is the presence of at least two transistors and at least one positive feedback loop".

With this understanding, all transistor circuits with two or more transistors and at least one positive feedback loop will be classified as being vulnerable to the harboring PAAST Trojans. Correspondingly, transistor circuits with only one transistor or with two or more transistors but no positive feedback loops are not vulnerable to harboring a PAAST Trojan.

Even a PAAST vulnerable circuit that is designed well with only one operating point can often be modified by simply changing some device sizes in such a way that the desired operating mode is maintained but an additional stationary equilibrium point that carries the Trojan is introduced and this additional operating mode can be extremely difficult to detect [25]. And, with this modification, the circuit may still perform well when operating at the desired equilibrium point. Another interesting but troublesome characteristic of some PAAST vulnerable circuits is that they can be designed in such a way that supply voltage or operating temperature changes add one or more Trojan states.

2.1 The Existence of Multiple States in Analog Circuits

2.1.1 The vulnerability of multiple operating points/modes in analog circuits

It is widely known that a circuit comprised of two back-to-back connected inverters, shown Figure 2-1, is often intentionally designed so that it is bi-stable. If designed to be bi-stable, the two stationary equilibrium points can be designated by the Boolean values of "0" and "1". As shown in the figure, the circuit has no inputs and two outputs labeled as Q and

Q'. Q will take the value which happens to be when it is powered up. For example, if Q='0' when the circuit is powered on, then Q'='1'. Correspondingly, if Q='1' when powered on, then Q'='0'. When designed to be bistable, the circuit has three equilibrium points. Two of these are stationary (alternatively stable), and one is quasi-stable. When operating near the quasi-stable operating point, the back to back connected inverters form a positive feedback loop.

An implementation of this circuit was designed in an IBM 0.13 um CMOS process. In this implementation, the inverters were comprised of the standard two-transistor architecture with an n-channel pull-down device and a p-channel pull-up device. The break-loop continuation method discussed in [26] can be used to obtain the equilibrium points. When the dc input impedance at the break point in the loop is infinite, the issue of loop loading when breaking the loop for determining static operating points is not of concern. Since the dc input impedance of the CMOS inverters is infinite, the loop can be broken at either the input of INV1 or the input of INV2. In Fig. 2-2 (a) the loop has been broken at the input to INV2. The loop transfer characteristics (often termed the return map) of the relationship between V_{OUT} and V_{IN} are shown in the figure. With the break-loop method, the equilibrium points of the circuit are at the intersection in the V_{OUT}:V_{IN} plane of the loop transfer characteristics V_{OUT} and the line showing V_{IN}. Simulation results showing the return map and the V_{IN} line for an implementation of this circuit are shown in Figure 2-2 (b). As expected, it can be observed that there are three intersection points. Points A and C are the two stationary equilibrium points and point B is a quasi-stable equilibrium point.

The stable and quasi-stable operating points can be compared to those of a ball on a symmetrical hill as shown in Figure 2-2(c) [27]. As described in Figure 2-2(c), 'A' and 'C'

are two stable operating points while ‘B’ is a quasi-stable operating point. For both the two-inverter loop and the “ball-on-the-hill” analogy, any slightly deviation from the quasi-stable operating point will cause the output to go to one of the two stable operating points if the time-dependent dynamics are included in the system models.

Sometimes the quasi-stable operating point is referred to as an unstable operating point. In the case of the two-inverter loop, the quasi-stable operating point in the static circuit corresponds to an unstable operating point in the dynamic two-inverter loop.

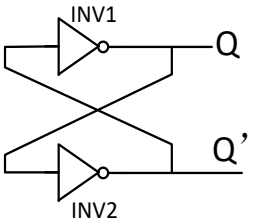


Figure 2-1 Back to back connected inverters

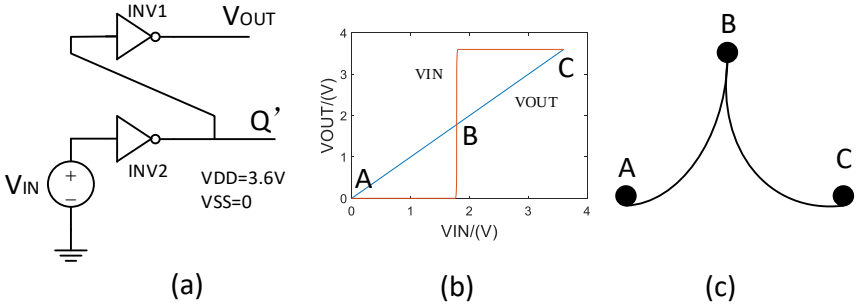


Figure 2-2 Three operating points exist in the back to back connected inverters

The back to back connected inverter circuit is intentionally designed to take advantage of the two stationary equilibria that can be used to store Boolean data. However, in some other circuits which are designed to operate at only one state but that may be unintentionally bistable or even have more than one additional stationary equilibrium point,

the extra state or states can be viewed as a Trojan state or states in the circuit. When operating in a Trojan state, the performance of the circuit may differ substantially from what is desired.

The existence of multiple equilibrium points in many nonlinear circuits is a mathematical property of these systems. Furthermore, multiple solutions can exist for some sets of nonlinear equations that arise in even relatively simple transistor circuits. This nonlinearity is inherently inherited from the nonlinearity of transistors. Cover for Trojans is embedded in the open problem that can be simply stated as "There is no known method for obtaining all solutions for a set of nonlinear equations in finite time". One might be tempted to argue that a good circuit simulator, such as SPICE or SPECTRE, or an equation solver in a program such as MATLAB could be used to obtain the solutions of a circuit. Unfortunately, these simulators or other computational tools only provide a single solution and their capabilities are inherently limited by the unsolved open problem of finding all solutions of a set of nonlinear equations. Consequently, if a nonlinear circuit has an undesired stationary equilibrium point that serves as a Trojan, it may escape detection in both the design and verification steps involved in the production of integrated circuits.

Even if only one state exists with the designed device sizes, nominal process parameters, nominal supply voltage, and nominal operating temperature, multiple states may still exist if changes occur in process parameters, supply voltages, or temperature. In the back to back connected inverters, the circuit is invariably designed so that two stationary operating points exist across worst-case variations in process, temperature, or supply voltage. Some good analog circuit designers who may also be Trojan creators may create a Trojan that would only have an undesired operating state for a specific supply voltage range or

temperature range. Such a circuit would pass all simulation and test criterion except when operating in the specific range but would still contain the Trojan. Since the undesired operating state would exist only for specific conditions, the simulator or other test tools would not detect it unless simulated/tested under the specific conditions. Furthermore, even if the circuit was simulated/tested under the vulnerable conditions, the undesired stationary operating state would only appear if it were specifically triggered. Unless the undesired operating state was present and triggered, there would be no abnormal signatures in any power domains or timing paths. Once this kind of Trojan is inserted into a circuit, it can be very difficult to detect.

Up to this point, emphasis has been placed on the static performance of a circuit and on the presence or absence of undesired stationary operating points. All integrated circuits also have energy storage elements embedded in the circuits. Often these energy storage elements are primarily parasitic capacitors, but parasitic inductors and non-parasitic capacitors and inductors are often present as well. When transistors are present, the nonlinearities in the transistors create nonlinear dynamic systems and these can be mathematically characterized with a set of nonlinear differential equations. If the time-dependence of the energy stored on the energy storage elements is neglected, this set of nonlinear differential equations can be reduced to a set of nonlinear static equations. Much like a set of nonlinear static equations, there are no known methods for obtaining all solutions for a set of nonlinear dynamic equations. But in contrast to the solutions of a set of nonlinear static equations which are points in a real number space, solutions of a set of nonlinear differential equations may be points in a real number space or may be time-dependent signals such as those that may come from waveform generators. The solutions

become even more complex if the inputs to a set of nonlinear differential equations are time-varying. But like the static operation of a nonlinear circuit, undesired stationary solutions of a nonlinear dynamic circuit may exist, and these solutions can be dramatically different from the desired solutions. And much like the static operation of a circuit, the undesired dynamic modes of operation can be viewed as the results of a Trojan in the dynamic operation of a circuit. And since the presence of undesired dynamic modes of operation can be created without affecting power, area, or circuit structure or without leaving any signatures in any power domains or signal paths, the Trojans that create the undesired dynamic modes of operation can also be termed PAAST Trojans.

In some digital Trojan related papers, reference is made to using analog circuits as a part of a trigger mechanism or as a payload [28]. The analog properties or additional analog circuits are used to change the signal or some delay characteristics, thus changing the Boolean output signal of the digital circuits. In [28], mention is also made of creating analog Trojans though no details are presented. Other authors have suggested creating analog Trojans by modifying or adding components to an analog circuit. Much like most digital Trojans that are discussed, such analog Trojans would alter circuit structure, layout area, and likely leave traces of their presence in some power domains or signal paths.

2.1.2 The identification of circuits with positive feedback loops

Trajkovic [29] and Green [30] observed that circuits with multiple equilibrium points also have feedback loops and under certain conditions, the presence of at least one feedback loop is a necessary but not sufficient condition for a transistor circuit to have more than one stable equilibrium point. Following the conventional wisdom stated previously, circuits with one or more positive feedback loops are vulnerable to the existence of multiple stationary equilibrium points. Thus, a method for identifying circuits that are vulnerable to the presence

of multiple stationary equilibrium points comprises identifying if at least one positive feedback loop is present in the circuit. And circuits without any feedback loops or with only negative feedback loops are not vulnerable to harboring a PAAST Trojan.

In [22], Willson shows that a circuit with two cross-coupled bipolar transistors creating a feedback loop is vulnerable to the existence of more than one operating points. Although Willson does not classify this cross-coupled feedback as "positive feedback", the specific cross-coupling is typically viewed as positive feedback. Though the term "positive feedback" in the context of circuits is widely used, a rigorous well-accepted definition of a positive feedback loop in a circuit appears to be lacking in the literature. Some authors have made mappings of a circuit to a graph and defined feedback loops and positive feedback loops in the corresponding graph. However, there are multiple mappings of circuits to graphs that have been used for various purposes and mapping a circuit to a graph invariably results in a loss of circuit information, thus raising questions about whether information relating to feedback or more specifically positive feedback is retained in a specific graphical representation.

A systematic positive feedback loop identification method was proposed in [31]. In this approach, a circuit with passive components, diodes, independent sources, and MOS transistors was mapped to a signed directed dependency graph (DDG). Each directed dependency is assigned a value of either "positive" or "negative". By using graph theory concepts and the dependencies between "branch currents" and "controlling voltages" which are defined in [31], positive feedback loops can be identified. A positive feedback loop is a loop with an even number greater than or equal to 2 of negative dependencies. Circuits with

one or more positive feedback loops in their signed DDG are said to be vulnerable to harboring PAAST Trojans.

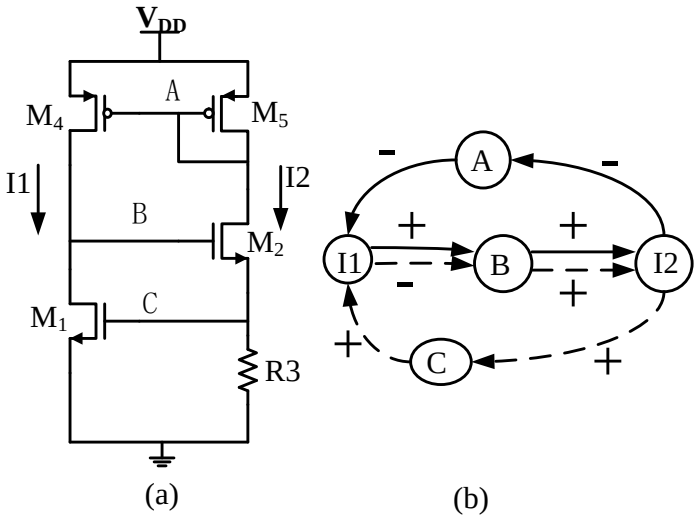


Figure 2-3 Loop identification on Wilson circuit; (a) Wilson circuit; (b) one positive feedback loop and one negative feedback loop

A Wilson bias generator circuit is shown in Figure 2-3 (a). By using the method introduced in [31], two loops are identified in the corresponding DDG as shown with dashed and solid lines in the node link diagram of Figure 2-3 (b). Since the number of the negative signs associated with the loop A→I1→B→I2→ is an even number, it is a positive feedback loop. Correspondingly, since the number of the negative signs associated with the loop C→I1→B→I2→C is an odd number, it is a negative feedback loop. The DDG for the Wilson circuit has only one positive feedback loop, thus, the break-loop continuation method can be used to find all operating points. Since the number of equilibrium points may be temperature dependent, it is necessary to do the break-loop analysis at all temperatures that are of concern.

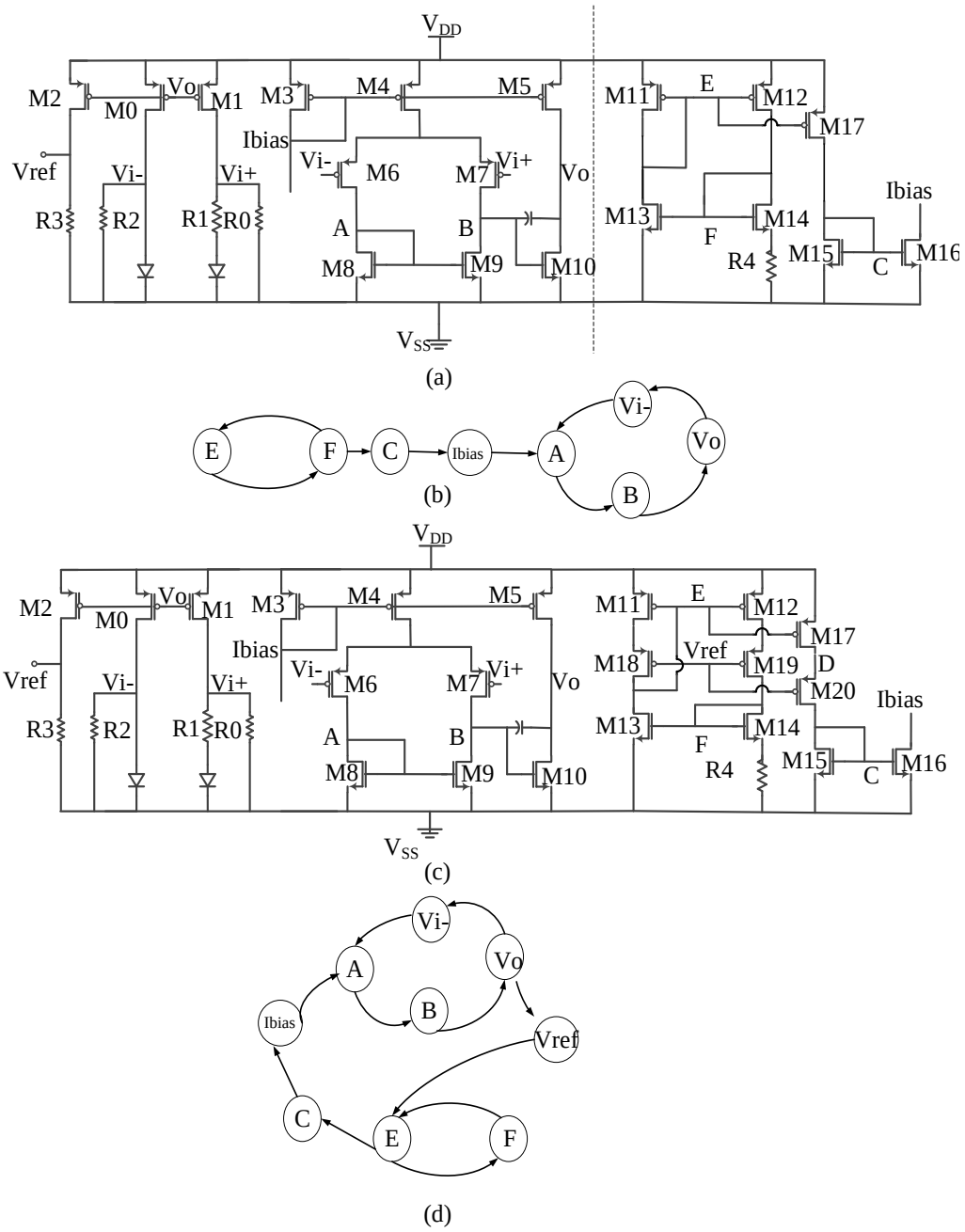


Figure 2-4 Loop identification circuits with two or more positive feedback loops (a) bandgap circuit with self-basing circuit; (b) node-link diagram for DDG of the circuit in (a)showing positive feedback loop; (c) bandgap circuit with cascode self-basing circuit; (d) node-link diagram for DDG of circuit in (c) showing positive feedback loop

Circuits with multiple positive feedback loops or coupled feedback loops can also be identified by the method introduced in [31]. Example circuits with multiple positive feedback

loops include some self-biased bandgap generators. Two bandgap circuits with different self-biased circuits are shown in Figure 2-4. The identification of positive feedback loops in the DDG of the circuits in Figure 2-4 (a) and Figure 2-4(c) are shown in the node-link diagrams in Figure 2-4 (b) and Figure 2-4(d), respectively. The two graphs are simplified to show only positive feedback loops and node voltage dependencies. As shown in Figure 2-4 (b), the circuit in Figure 2-4 (a) has two positive feedback loops, and the loop A→B→Vo→Vi-→A has one directional dependency from loop E→F→E. The circuit in Figure 2-4 (c) is a modified version of circuit in Figure 2-4 (a). In Figure 2-4 (c), the biasing circuit has a cascode structure and the 'Vref' of the bandgap circuit is connected to the gate of the cascode transistors, which generates one more positive feedback loop as shown in Figure 2-4 (d). The positive feedback loops of the circuit in Figure 2-4 (c) are coupled together and more complex. To verify the presence of multiple equilibrium points on these circuits by breaking loop method, multiple nodes need to be broken. The high dimensional computation makes the breaking loop method not practical or inefficient on circuits with two or more positive feedback loops, not to say to obtain the temperature range where multiple equilibrium points exist.

2.2 Benchmark of PAAST hardware Trojans in analog circuits

Analog circuits are circuits in which the continuous-values of voltages and current are of interest in contrast to digital circuits where the variables of interest are typically associated with one of two discrete levels. Analog circuits are often built with resistors, inductors, capacitors, MOS transistors, and bipolar transistors. Amplifiers, reference generators, oscillators, filters, and other important and fundamental circuits are classified as analog circuits. In analog circuits that include transistors, nonlinearity is almost unavoidable due to

the inherent nonlinearity of the transistors themselves. Nonlinearities can also be introduced through the nonideal characteristics of actual resistors, inductors, and capacitors.

It is known that circuits with positive feedback loops in the DDG are vulnerable to multiple equilibrium points. Positive feedback loops exist in many commonly used basic analog circuits such as reference generators, temperature sensors, self-stabilized bias generators, and some power management circuits. It is also known that some nonlinear analog circuit supports more than one stationary dynamic mode of operation. Multiple dynamic modes of operation have been reported in several types of analog circuits including filters, PLLs, oscillators. These multiple dynamic modes of operation are inherently associated with the nonlinearity of devices as well. Though there has been some work reported on identifying vulnerability of a static circuit to the presence of undesired stable equilibrium points, specifically relating to architectures that have positive feedback loops in a corresponding DDG, there is little in the literature that focuses on the vulnerability to the presence of multiple stationary dynamic modes of operation. However, as examples show, nonlinear analog circuits can also support undesired dynamic modes of operation and these circuits are also PAAST. In this section, several example circuits will be presented that support either multiple static modes of operation or multiple dynamic modes of operation. These will serve as benchmark circuits that are useful for studying characteristics of, vulnerability to, and methods of preventing the introduction of PAAST Trojans into useful analog circuits.

2.2.1 Analog hardware Trojans in static circuits

2.2.1.1 Analog hardware Trojan in Inverse Widlar circuit

A circuit shown in Figure 2-3(a) can be used as a bias current reference generator is discussed in [32]. This is often termed the Wilson bias generator. It possesses a single positive feedback loop in the DDG and the Trojan which can be inserted into this circuit has the PAAST properties. This will serve as the first benchmark circuit. In some implementations, it exhibits two stable equilibrium modes over a designer-controlled temperature range. The undesired stable equilibrium point can be a Trojan state and can be very difficult to detect since it may be present only over a limited temperature range. In [33], the existence of multiple stable equilibrium points in the inverse Widlar circuit, which is often used as a voltage reference generator or temperature sensor, is discussed. This circuit is shown in Figure 2-5 and serves as the second benchmark circuit.

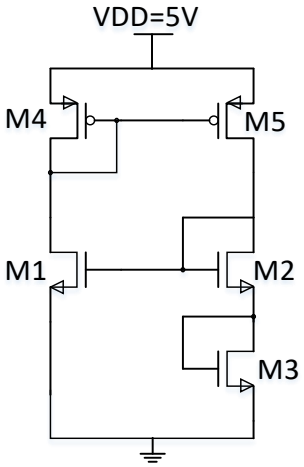


Figure 2-5 Inverse Widlar circuit

In both of these benchmark circuits, with only a small change in component values, the temperature ranges where Trojan equilibrium points exist can change from a wide range to a very narrow range. A detailed discussion of temperature signatures of circuits with multiple equilibrium points is presented in Chapter 2.4.

2.2.1.2 Analog hardware Trojan in Bandgap circuit

Much like the circuits in [32]-[33], the commonly used bandgap reference generator circuit of Figure 2-6, first published by Banba [34], can have two stable equilibrium points if an effective start-up circuit is not included. This will serve as the third benchmark circuit. Since the desired output voltage Vref is temperature insensitive, it is often used as a reference generator.

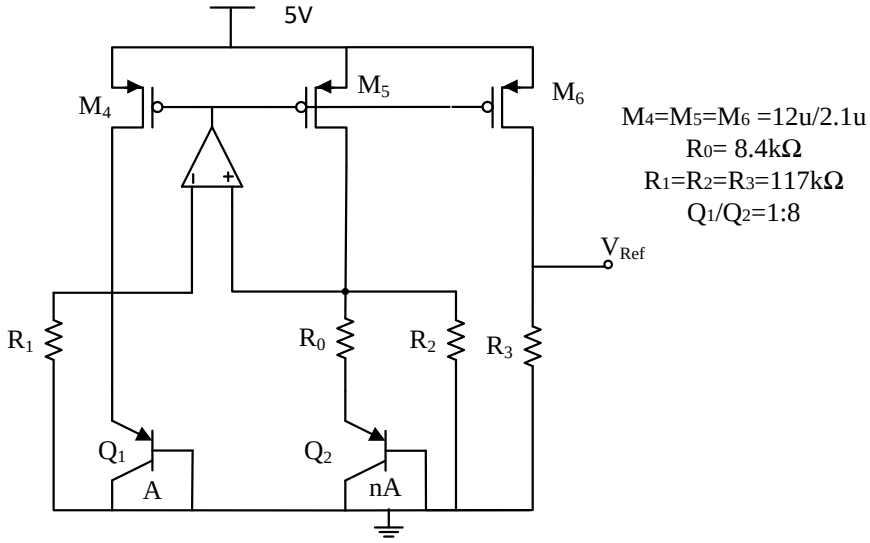


Figure 2-6 Bandgap reference circuit

Though originally proposed for operation at low supply voltages, the Banba reference can be designed to provide a wide range of nominal output voltages. An implementation of this circuit in the 0.5u ON CMOS process designed to operate with a Vref of 1.25V using the components listed in Figure 2-6 was designed. Simulation results obtained from a bi-directional temperature sweep, which is explained in more detail in Chapter 3, are shown in Figure 2-7. These simulation results show a hysteresis window in the temperature domain over the 70℃ to 200℃ interval. Over this interval the circuit has two stable equilibrium points, one is the desired operating point at approximately 1.25V and the other is a Trojan

operating point at a very low output voltage. Even if the circuit is operating at the desired output, it can be triggered to the Trojan state either intentionally or accidentally. As can be seen from the simulation results, the circuit actually has three solutions over the 70℃ to 200℃ interval with the intermediate point corresponding to the asterisk line being an unstable equilibrium point. Irrespective of whether the undesired stable operating point at a given temperature is inserted accidentally or intentionally by designers, the operation of the circuit at the undesired operating point is dramatically different from that at the desired equilibrium point.

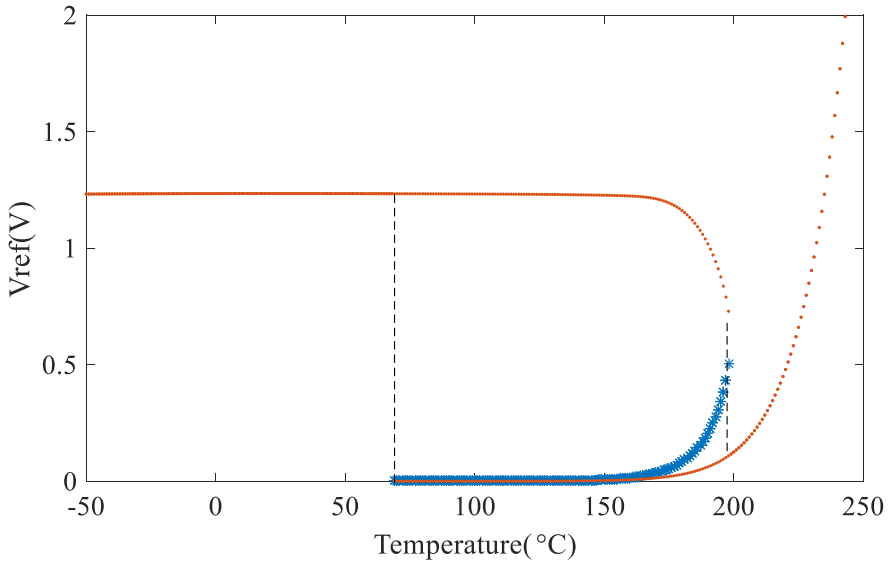


Figure 2-7 Operating points of bandgap reference circuit VS temperature

The existence of the undesired operating point in the Banba bandgap circuit, as well as several other well-known bandgap circuits, is well known and “start-up” circuits are often used to remove the undesired equilibrium state. However, since the multiple operating points are process, voltage, and temperature (PVT) dependent, it is often not easy to verify the robustness of some start-up circuits. In only slightly more complicated circuits, it can be

difficult to even recognize that the circuit may have multiple stable equilibrium points and it is these circuits that are vulnerable to the adversarial insertion of Trojan analog states.

In static analog circuits with PAAST Trojans, the payload is often viewed as operation of the circuit at an undesired stable equilibrium point. If the bandgap circuit in Figure 2-6 serves as the reference for the ramp waveform generator shown in Figure 2-8, the payload associated with a multi-stage Trojan in the bandgap circuit is a change in the operating frequency of the waveform generator. This will serve as the fourth benchmark circuit.

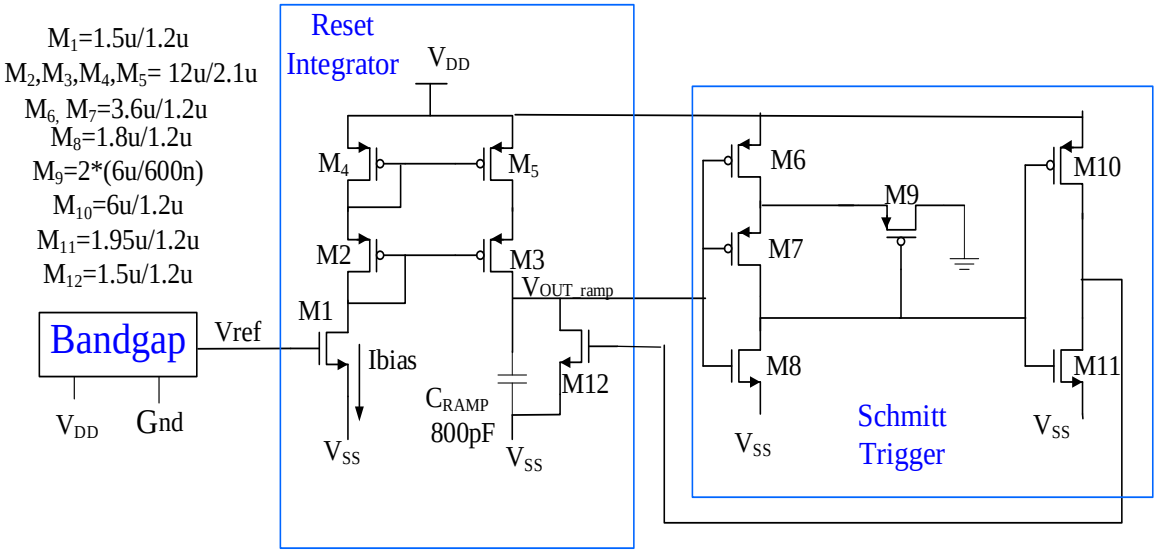


Figure 2-8 one ramp oscillator circuit

The waveform generator circuit is comprised of three blocks, a bandgap circuit, a reset integrator, and a Schmitt trigger circuit. The 'Vref' of the bandgap circuit is temperature insensitive, and it is used as a bias voltage to generate a constant current in M1. The bandgap circuit is referenced to ground instead of VSS and thus for appropriate values of VSS will generate two different non-zaro bias currents in the reset integrator depending upon which state the bandgap circuit is operating in. The Schmitt trigger circuit has a hysteresis window

which is bounded by two voltages V1 and V2 (VSS<V1<V2) . When the input voltage '$V_{OUT_{ramp}}$' of the Schmitt trigger is lower than V1, M12 is off and the current mirror output in the integrator will charge C_{RAMP} linearly until the voltage on the capacitor reaches to V2. When the input signal of the Schmitt trigger increases to V2, the gate voltage of M12 will go high and cause transistor M12 to dischargeC_{RAMP}. If the transistor M12 has a low ON impedance, the discharge will be rapid and $V_{OUT_{ramp}}$ will drop quickly to VSS. The drop in $V_{OUT_{ramp}}$ will reset the Schmitt trigger and the process will repeat thus resulting in a saw tooth periodical waveform on $V_{OUT_{ramp}}$. The oscillating signal's magnitude and frequency are determined by V1, V2, C_{RAMP} , and the two values of Ibias.

If the difference between 'Gnd' and 'VSS' is sufficiently small, one of the values of Ibias will be 0 and when the circuit operates in this mode, oscillation will cease. Thus, depending on the value of VSS, the extra stationary mode of operation can be either a different oscillating frequency or an extra static operating state.

Simulation results for an implementation of this circuit in the same 0.5u ON CMOS process and using the bandgap bias generator of Figure 2-6, operating at 75℃ with supply voltages of VDD=5V and VSS=0V, are shown in Figure 2-9. For this implementation, the circuit has two stationary modes of operation. One is the desired saw ramp oscillating mode which has an oscillation frequency of 2.82 KHz and the other is the Trojan state corresponding to an undesired constant static operating state.

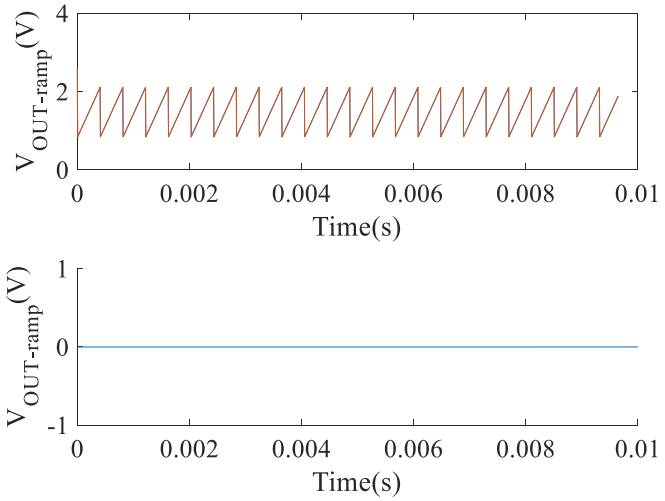


Figure 2-9 The desired ramp oscillating state and one static Trojan state

Thus, in this example, the payload of the Trojan for sufficiently negative values of VSS would be a second undesired operating frequency or for less negative values of VSS, the payload would be failure of the oscillator to oscillate. In the latter case, depending upon the application, the payload could be viewed as a denial of service. But in either case, when reset, the desired mode of operation would resume.

2.2.2 Analog hardware Trojans in second-order dynamic circuits

The benchmark circuits introduced in the previous section can all harbor a Trojan in the static operation of the circuit. But as the previous example showed, a Trojan static mode of operation of a subcircuit can also affect the dynamic performance of a circuit. However, the dynamic performance of a circuit can also be altered with a PAAST Trojan more directly without having multiple static modes of operation in a subcircuit. The equations characterizing the operation of a circuit can be static nonlinear or time-differential nonlinear equations. The solutions of sets of nonlinear static equations are often termed static

equilibrium points. Correspondingly, the solutions of sets of nonlinear time-differential equations can be either static equilibrium points or dynamic modes of operation.

Similar to the multiple operating points that can exist in static nonlinear analog circuits, multiple stationary operating modes can also exist in the dynamic nonlinear circuits. One such example is an analog filter circuit that has two stationary dynamic outputs with different amplitudes for one fixed periodic input signal. Another example is an oscillator circuit that has two stationary oscillating states with different amplitudes or different frequencies. The undesired modes of operation in dynamic nonlinear circuits are also termed Trojan modes.

Transient simulations with standard circuit simulators can help designers observe dynamic modes of operation of a nonlinear circuit. However, simulators invariably provide only one operating mode with a single transient simulation. The mode of operation provided by the simulator for a transient simulation is determined primarily by the initial conditions set at the beginning of the simulation or possibly, on occasion, by other circuit components or elements that "numerically" couple into the transient equation solver. Trojan dynamic modes of operation in a circuit can be very difficult to observe with a standard transient simulation and often require setting initial conditions very close to an operating mode in the Trojan operating mode of the circuit. Even if it is known that a Trojan operating mode exists, it can be difficult to verify the mode with transient simulations unless appropriate initial conditions are set. And, the problem of finding a dynamic Trojan operating mode or Trojan operating modes can be even more challenging if it is not known whether or not one or more Trojan operating modes actually exist. In the following section, examples of Trojans in dynamic nonlinear circuits that can serve as benchmarks will be given. Much like the vulnerability to

embedding static Trojan states in basic static analog circuits, Trojan dynamic operating modes with PAAST characteristics can be easily embedded.

2.2.2.1 Analog hardware Trojan in Wein bridge oscillator circuit

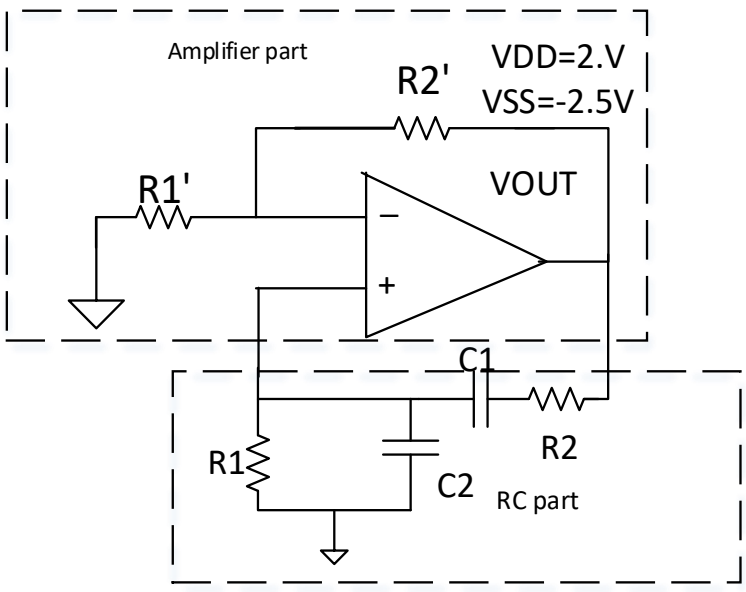


Figure 2-10 Wein bridge oscillator

The Wein bridge oscillator has been used for decades. The basic Wein bridge oscillator contains one OPAMP, four resistors, and two capacitors as shown in Figure 2-10. The OPAMP and the resistors R1' and R2' form a finite gain amplifier. Any oscillator circuit requires a nonlinear component to control the oscillation amplitude and spectral performance. In the Wein bridge oscillator, diodes or transistors are widely used to add some nonlinearity to the finite gain amplifier subcircuit. Transistors are often used in the SOC level designs for adding the nonlinearity whereas diodes are often used in board-level designs. Similar to the multiple static states that may exist in static nonlinear circuits, multiple dynamic modes may occur in nonlinear dynamic circuits under some specific feedback conditions. In the Wein Bridge oscillator, the path containing the capacitors and the two resistors R1 and R2 form a feedback path to the non-inverting input of the OPAMP.

The feedback factor of the finite-gain amplifier can be defined by Equation (2-1)

$$\theta = \frac{R1'}{R2' + R1'} \tag{2-1}$$

The gain of the finite-gain amplifier is $K = \frac{1}{\theta}$. If the operational amplifier is ideal and if R1=R2=R and C1=C2=C, the characteristic equation for the Wein bridge oscillator is given by Equation (2-2).

$$D(s) = s^2 C^2 R^2 + sCR(3 - \frac{1}{\theta}) + 1 \tag{2-2}$$

If θ is smaller than $\frac{1}{3}$ (correspondingly the gain K is larger than 3), there are complex-conjugate poles in the right half-plane, which makes the circuit unstable and thus induces oscillation that will grow in amplitude without bounds. Correspondingly, if θ is larger than $\frac{1}{3}$ (correspondingly K is less than 3) , the poles are in the left half-plane and the circuit is stable. But the OPAMP is not ideal and essentially all OPAMPs will saturate when the outputs approach VDD or VSS. If the finite amplifier gain is very linear and modestly larger than 3 before saturation at VDD and VSS, the circuit will oscillate and have one oscillation mode but with severe distortion due to the OPAMP saturation near VDD and VSS. Different nonlinearities can be added to the finite amplifier with diodes and resistors to limit the gain K to a value that is less than 3 as the output amplitude of the finite gain amplifier approaches VDD or VSS. By judiciously managing the finite gain by intentionally introducing nonlinearity in the finite gain amplifier, the hard saturation near VDD and VSS can be eliminated and distortion in the output of the Wein bridge oscillator can be reduced. Good circuit designers invariably use this approach to reduce distortion.

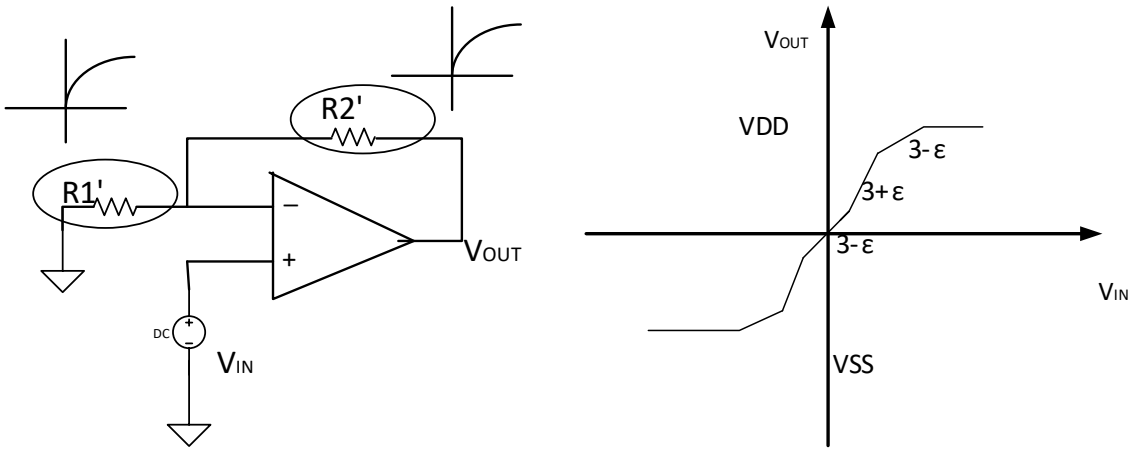


Figure 2-11 Soft nonlinearities in the amplifier

However, some nonlinearity that may be introduced to reduce distortion can also create additional stationary operating modes. If the resistors, diodes and/or transistors connected in a way which makes the transfer characteristics of the amplifier nonlinear such as shown in the right part of Figure 2-11, at least two different stationary modes of operation can occur.

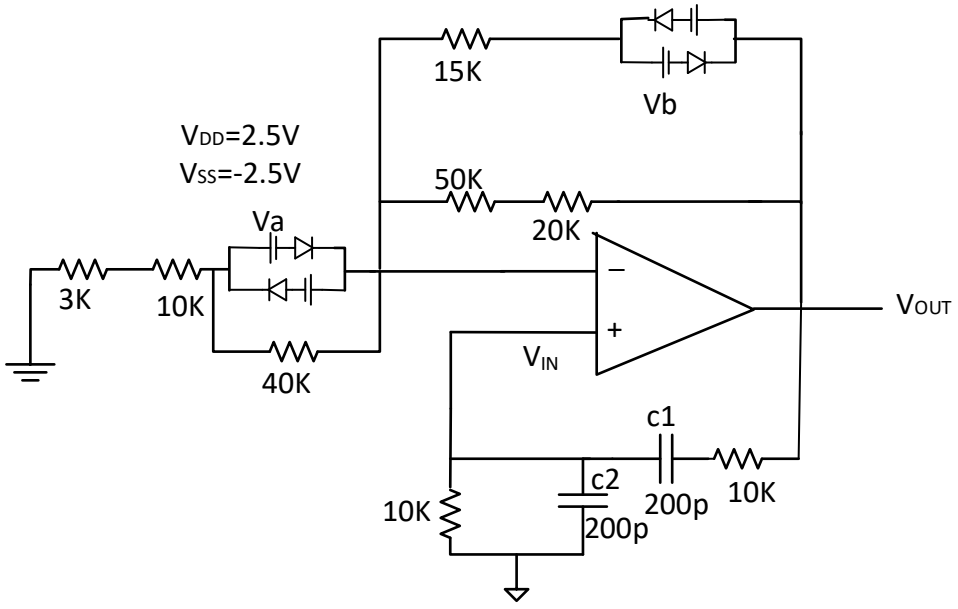


Figure 2-12 Wein Bridge Oscillator with one static Trojan state

The modified circuit including all component values is shown in Figure 2-12. This circuit serves as the fourth benchmark circuit. The OPAMP was still assumed to be ideal. Simulation results for this circuit are shown in Figure 2-13. In the first simulation, the initial conditions on the capacitors C1 and C2 were set at 0 V and 0 V respectively. In the second simulation the initial conditions were set at 2.5 V and 2.5 V respectively. It can be observed from Figure 2-13 (a) that when the initial conditions on C2 and C1 are low, the circuit will not oscillate and VOUT will stay at a stable constant voltage. However, when the initial conditions added at the two capacitors are higher, the circuit will start to oscillate, as shown in Figure 2-13(b). In this example, the oscillator has two operating modes, of which one is a stable static mode while the other is a dynamic oscillating mode. If the initial condition range to have the circuit converge to the static mode of operation is very small, it will be difficult to detect this mode even with many transient simulations. Furthermore, if the circuit with this static mode is used to generate periodic waves for other circuits, while some environment condition changes which accidentally trigger this static mode, the whole functional circuit may fail to work. So, for the oscillator, one kind of Hardware Trojans is that the oscillator has multiple operating modes and one of them is a static mode which will totally stop the function of the circuit. This Trojan has the basic properties of a PAAST Trojan.

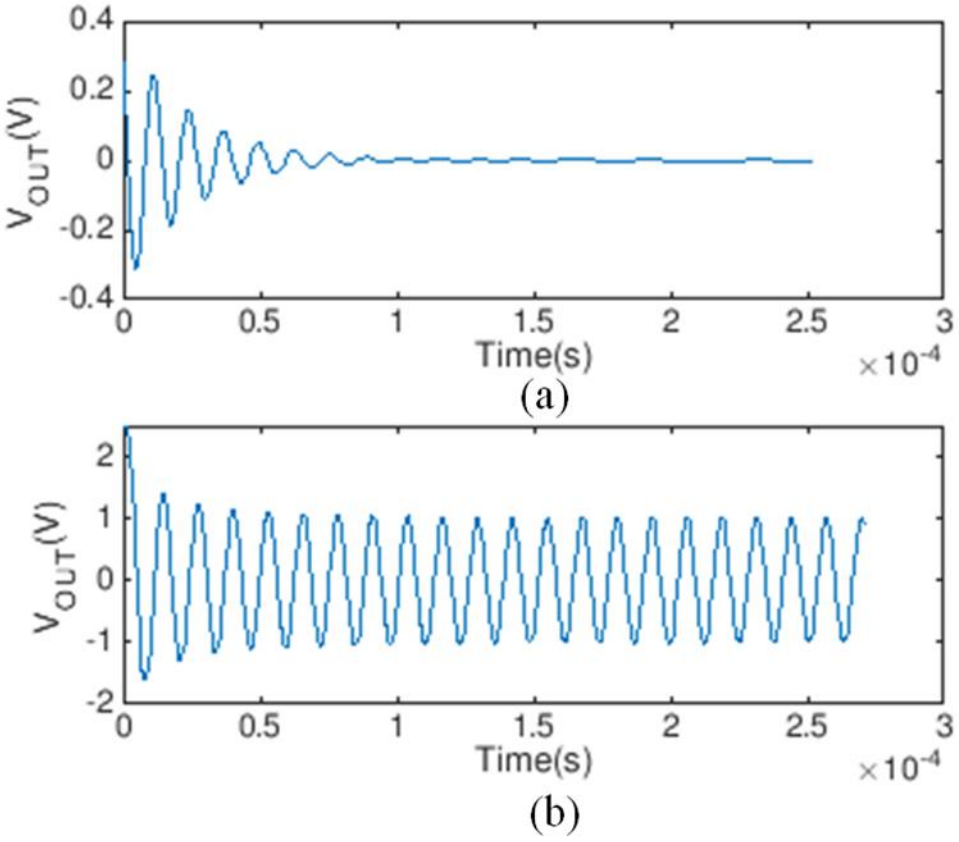


Figure 2-13 Two states of the oscillator with amplifier in Figure 2-12 at different initial conditions; (a) initial conditions on C1 and C2 is 0V and 0V; (b) initial conditions on C1 and C2 is 2.5V and 2.5V.

Another type of dynamic analog Hardware Trojans in an oscillator is one that has more than one oscillating mode and all modes have different oscillating frequencies or different oscillating amplitudes. If the resistors, diodes, or transistors are connected in such a way that creates transfer characteristics of the finite gain amplifier with the nonlinear characteristics shown in Figure 2-14, two different stationary oscillating modes of the oscillator will be created. A schematic of an implementation of the Wein bridge oscillator that includes this nonlinearity is shown in Figure 2-15. Simulation results for this circuit for two different set of initial conditions are shown in Figure 2-16. The OPAMPs were assumed to be ideal in these simulations. Both simulation results represent stationary modes of

oscillation. In the first simulation the initial conditions on the capacitors C1 and C2 were set at 0.1 V and 0.1 V respectively. In the second simulation the initial conditions were set at 2.5 V and 2.5 V respectively.

In the first simulation the frequency of oscillation was around 80 KHz and amplitude (peak value) was 0.4V. In the second simulation which corresponded to larger initial conditions on the two capacitors, the frequency was same around 80 KHz and the amplitude was 2.5V. Note that the two oscillation frequencies are similar but the amplitudes are significantly different. Though not shown here, the spectral characteristics of the two waveforms are also quite different. The circuit of Figure 2-15 serves as the fifth benchmark circuit.

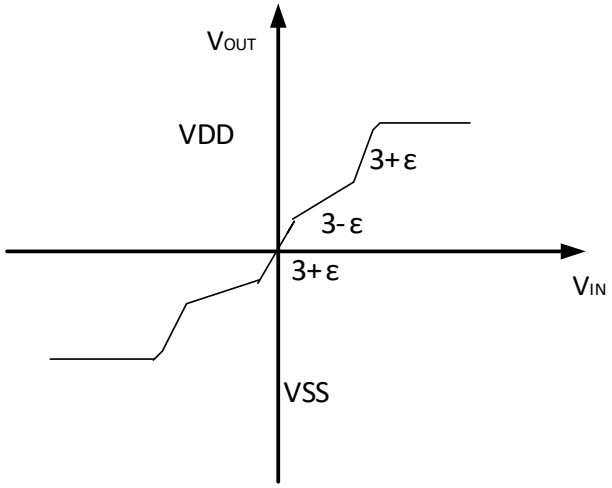


Figure 2-14 Another kind of soft nonlinearities in the amplifier

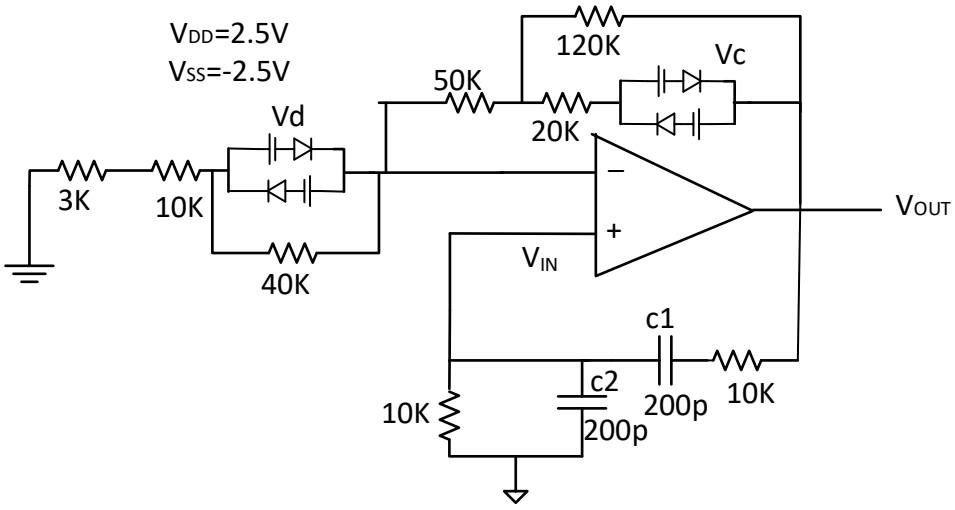
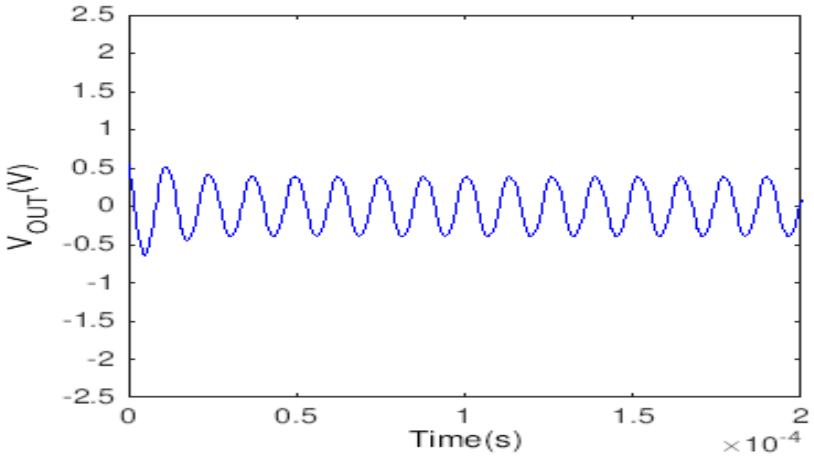


Figure 2-15 Wein Bridge Oscillator with one dynamic Trojan state

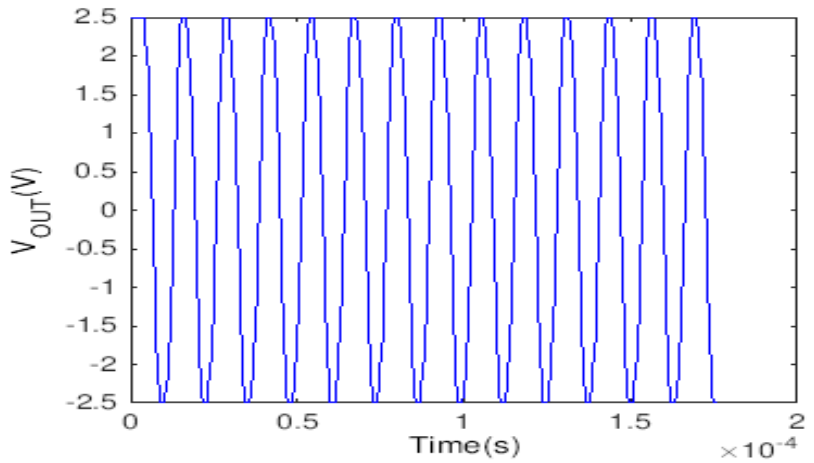
Though not a popular method for designing the Wein bridge oscillator, the nonlinearity could also be added to resistors R1 and R2 or the capacitors C1 and C2. If the nonlinearity is added at the RC part of the circuit while the amplifier has a constant gain, multiple stationary oscillating modes can also be observed under different initial conditions. In contrast to the nonlinearities in the finite gain amplifier part of the circuit which caused significant shifts in magnitude but only small changes in frequency, nonlinearities in the RC part cause significant changes in both amplitude and frequency.

Much like the challenges of detecting the presence of Trojan static operating modes, the initial condition domain of attraction for Trojan dynamic operating modes of operation can be very narrow making it difficult to observe the presence of a Trojan that creates an undesired dynamic mode of operation by changing the initial conditions in a transient simulation. Though the circuits with multiple dynamic modes of operation discussed in this section had only two energy storage elements, resulting in a two-dimensional initial condition domain, nonlinear circuits with more than two energy storage elements can also harbor dynamic PAAST Trojans. A circuit with 'n' energy storage elements would require

'n' initial conditions to completely manage a transient simulation and considering all possible initial conditions in a transient simulation would require exploring an n-dimensional initial condition domain. A well-disguised PAAST Trojan whereby the Trojan mode of operation had a domain of attraction that is small in an n-dimensional initial condition domain could be extremely difficult to detect yet could have devastating consequences if it were triggered.



(a)



(b)

Figure 2-16 Two oscillating states of the Wein Bridge oscillator; (a)initial conditions on C1,C2 are 0.1V;(b) initial condtions on C1, C2 are 2.5V

2.2.2.2 Analog hardware Trojans in Sallen and Key structure based filter circuit

Many filter circuits can harbor dynamic PAAST Trojans. In this section, two types of PAAST Trojans that can be embedded in Sallen and Key filter circuits [35] will be discussed. Emphasis will be restricted to a single second-order Sallen and Key structure though results could be readily extended to many other structures of varying orders. Since emphasis will be restricted to a single second-order structure, the results presented in this section are quite similar to those associated with the Wein bridge oscillator circuit.

A popular Sallen-Key bandpass filter structure is shown in Figure 2-17(a). If the resistors are equal and the capacitors are equal, that is, R_1=R_2=R_3=R and C_1=C_2=C, then the transfer function of this filter T(s), is given by Equation (2-3).

$$T(s) = \frac{K}{RC}\frac{s}{s^2+s\left(\frac{4-K}{RC}\right)+\frac{2}{(RC)^2}} \tag{2-3}$$

where K is the gain of the finite gain amplifier. The finite gain amplifier is typically created using an OPAMP and two resistors.

As shown in the Equation (2-3), when K is smaller than 4, the poles are in the left half-plane, which makes the circuit stable. However, if K is larger than 4, there are poles in the right half-plane and the filter will not perform as a stable filter. As in the Wein-bridge oscillator example, a nonlinearity can be added to the finite gain amplifier. If the transfer characteristics of the finite gain have the nonlinearity shown (exaggerated) in Figure 2-17(b), while the RC part of the filter circuit is ideal, two operating modes of the filter will occur for one time-domain input signal. This circuit will serve as the sixth benchmark circuit. Simulation results for sinusoidal input with p-p amplitude of 0.5V and frequency of 5K Hz for initial conditions of on C1 and C2 of 0 V and 0 V respectively are shown in Figure 2-18 (a). Simulation results with initial conditions on C1 and C2 of 2.5 V and 2.5V respectively

are shown in Figure 2-18 (b). Two substantially different output signals can be observed at the VOUT for different initial conditions. As expected, the output signals are both of the same frequency as the input signal but both the wave shape and the amplitudes of the outputs are substantially different.

A similar observation has been reported in other papers [36]-[39] where the phenomenon was referred to as the Jump Resonance of the filter. In the context of analog filters, the effects of jump resonance are often undesired and unanticipated and associated with modest nonlinearities that naturally occur in the analog circuit itself [39] though some authors have intentionally taken advantage of the jump resonance phenomena to build very sensitive detection circuits. Filters with jump resonance can have an abrupt voltage jump at the output node with small changes in the input signal's frequency and no change in the amplitude of the input signal. In such cases, instead of changing the mode of operation by changing the initial conditions, the mode of operation is changed can be changed by altering the input signal. Actually, jump resonance in a filter can be viewed as a hysteresis window in the frequency domain transfer characteristics obtained when the input sinusoidal signal's amplitude is fixed.

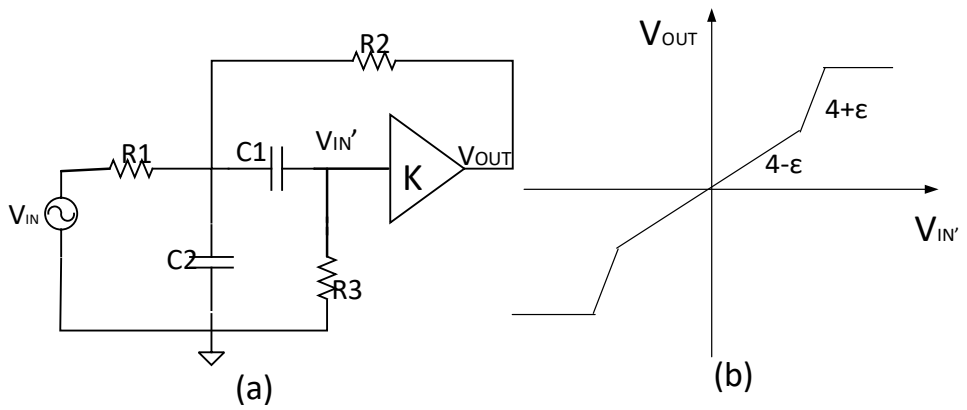


Figure 2-17 Sallen key bandpass filter and its nonlinearities in the amplifier

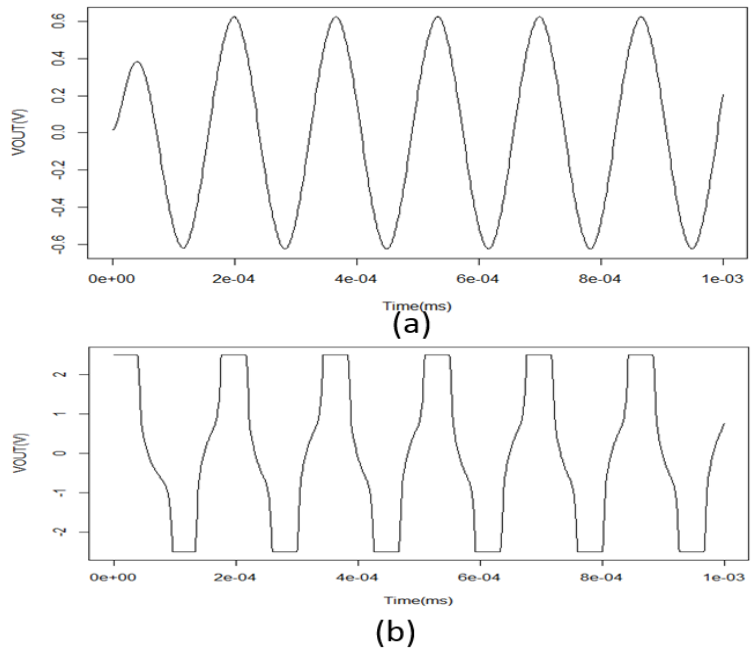


Figure 2-18 Two states of the filter with same input signal at different initial condtions

Thus, the multiple dynamic outputs of the filter can be viewed as the outputs associated with a PAAST Trojan. As with other PAAST Trojans, the range of amplitudes and frequencies over which jump resonance can occur can be very narrow making it difficult to detect the existence of this Trojan in a filter.

2.2.2.3 Analog hardware Trojans in Sallen-Key based oscillator circuit

It has been shown in the previous section that for modest nonlinearities in the finite gain amplifier, the Sallen and Key filter circuit can harbor a PAAST Trojan with a jump resonance payload. Specifically, for a given sinusoidal input signal with fixed frequency and fixed peak-to-peak amplitude, the circuit can have two stationary dynamic modes of operation. In the desired mode of operation, the output will be a sinusoidal signal with amplitude and phase scaled as predicted from the linear transfer function of the filter. In the Trojan mode, the output is more like a distorted square wave.

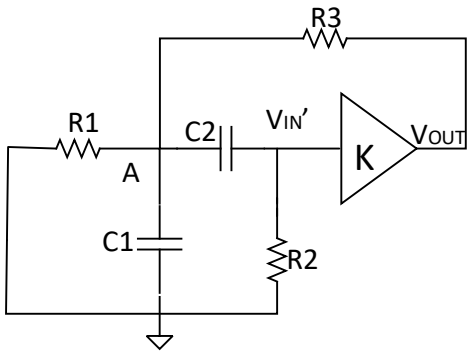


Figure 2-19 Oscillator based upon Sallen-Key structure with K=4

A Sallen-Key type oscillator can also be formed by adjusting the gain of the finite gain amplifier for the circuit of in Figure 2-17 to 4 and grounding the input as shown in Figure 2-19. The characteristic equation for this circuit under the assumption of linear operation for R1=R2=R3=R and C1=C2=C is given by Equation (2-4)

$$D(s) = s^2 + s\left(\frac{4-K}{RC}\right) + \frac{2}{(RC)^2} \tag{2-4}$$

Sinusoidal oscillation is achieved by placing the poles on the imaginary axis which will occur when K=4 ideally. In practice, a slight nonlinearity is introduced into the amplifier to control both amplitude and distortion of the oscillator output with a gain that is slightly larger than 4 for small-amplitude output signals and slightly less than 4 for large amplitude output signals. However, if an additional slightly nonlinearity region exists in the amplifier or in the resistor; an extra oscillating mode which will be a Trojan state can also exist.

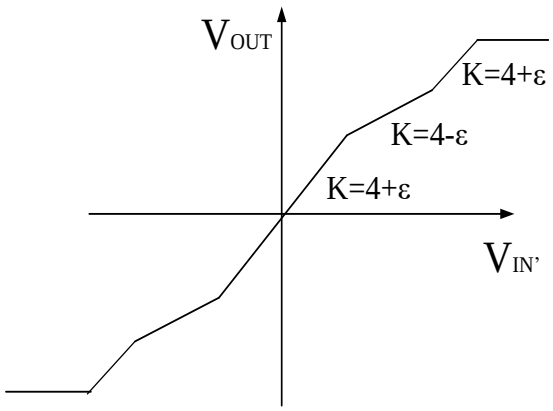


Figure 2-20 Nonlinearity in the gain of K amplifier

A specific nonlinearity of the finite gain amplifier that can be used in the Sallen and Key oscillator is shown exaggerated in Figure 2-20 . This can be considered as the seventh benchmark circuit. This oscillator was designed for generating a periodical sinusoidal signal with a frequency of around 560 KHz.

Simulation results for this circuit are shown in Figure 2-21 for two different initial conditions on the capacitors C1 and C2. In this simulation, the initial conditions on C1 and C2 were set at 0.1 V for the first simulation and at 2.5V for the second simulation. Simulation results showing the desired oscillation mode corresponding to the first initial condition is in Figure 2-21(a), while the Trojan oscillating mode corresponding to the second initial condition is shown in Figure 2-21(b). In the desired mode of oscillation, the output is nearly sinusoidal with an oscillation frequency of approximately 560 KHz signal and with amplitude of approximately 2V p-p. The Trojan mode of operation provides a highly distorted signal with amplitude in excess of 4V p-p. The frequencies of oscillation for the two stationary modes of operation are about the same.

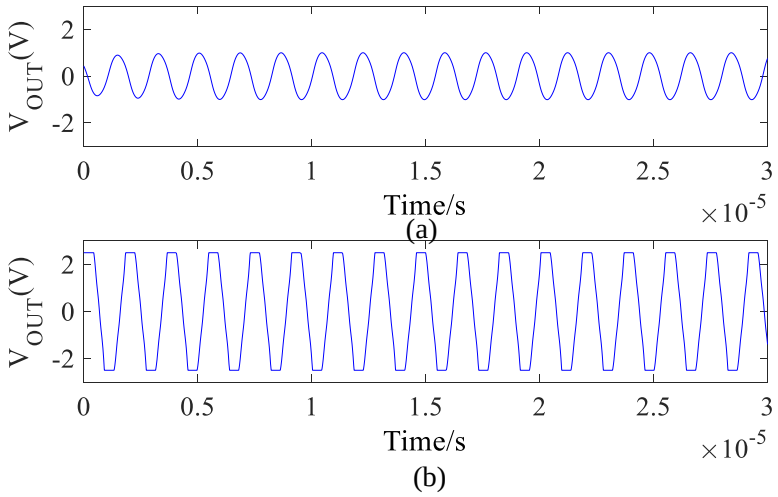


Figure 2-21 Stationary oscillating States of circuits with K in Figure 2-20

In the design of this circuit, the nonlinearities in the amplifier can be set so that the Trojan mode exists only over a small range of initial conditions, or over a large range of initial conditions. Regardless, this is also a PAAST Trojan.

Though the nonlinearity was introduced in the finite gain amplifier in this circuit, the RC part of the circuit can also have a signal magnitude dependent nonlinearity. As for the Wein bridge oscillator, by introducing the nonlinearity in the finite gain amplifier, both modes of operation resulted in about the same frequency of oscillation but significantly different magnitudes. Introducing the nonlinearity into the RC part of this circuit in such a way that two stationary modes of operation are obtained will cause a shift in frequency between the desired and Trojan modes of operation.

Though the examples presented here have focused on a single stationary dynamic Trojan mode where the characteristics of the Trojan mode are significantly different than those of the desired mode of operation, oscillators with multiple dynamic Trojan modes of operation have been observed where the frequency and amplitude are different in each Trojan

mode. Other oscillator circuits have been observed that exhibit an undesired stable static mode of operation. Though significant nonlinearities have been intentionally introduced in the dynamic benchmark circuits to introduce PAAST Trojans, even modest nonlinearities typical of those that more naturally occur can also create PAAST Trojans. Such Trojans can be introduced without making any changes in the circuit architecture and thus will escape essentially all proposed methods for detecting a hardware Trojan.

2.2.3 Analog Hardware Trojans in injection locked circuits

Generation of clock signals in integrated circuits that have a large number of digital gates is becoming an increasingly challenging problem since systematic and random path delays often introduce unacceptably large clock skew. Traditional clock distribution methods are based upon global H-Tree and local H-Tree networks which ideally can reduce clock skew to acceptable levels by balancing the length and parasitics of delay path with careful layout techniques. However, in emerging processes, higher clock rates, larger die sizes, wider busses, and increasing numbers of interconnect layers are making it increasingly difficult to meet skew requirements with traditional clock distribution methods. In recent years, there has been considerable interest in using synchronous distributed clock oscillators to locally generate clock signals. This approach offers potential for reducing the clock skew inherent with H-tree clock routing as well as attractive phase noise properties [40]-[42]. Invariably these clock-generation oscillators incorporate some level of injection locking and phase alignment to meet clock skew requirements. But these injection-locked clock generation networks can also harbor hardware Trojans and the Trojans that can be introduced in injection-locked clock generators are the focus of this section. Similar PAAST Trojans which have undesired states or equilibrium points in a static circuit or undesired modes of operation in a nonlinear dynamic circuit, injection locked clock generation circuits can also have extra

undesired mode of operation. In this section, three injection locked oscillators for clock generation purposes with PAAST Trojans are introduced as another three benchmark circuits.

The circuits are designed so that they normally operate as desired but when triggered, they switch to the Trojan mode of operation. The first injection locked oscillator which can be the eighth benchmark circuit is comprised of two injection locked 3-stage ring oscillators with complimentary outputs. During normal operation, injection locking is used to lock both to the same frequency. A stationary Trojan mode of operation, when triggered, causes both to operate at the same frequency but with in-phase outputs instead of complimentary outputs. When in the Trojan mode, the amplitude and frequency are also different from what is obtained in the desired mode. The ninth benchmark circuit is an injection-locked frequency divider [43]. It is comprised of two three-stage ring oscillators where one oscillates at a nominal frequency that is approximately twice that of the other. A flip-flop is used to divide the higher frequency by a factor of 2 to obtain a subharmonic output. The lower frequency oscillator output is injection-locked to the higher frequency oscillator thereby forcing the low frequency oscillator output to be at exactly half of the frequency of the higher frequency oscillator. In the desired mode of operation, the two lower-frequency outputs are in-phase. A Trojan mode of operation, when triggered, causes the two outputs to be 180° out of phase. The two outputs are of the same frequency and the same output amplitude as the desired signals. The tenth benchmark circuit is of a widely used quadrature oscillator where two voltage-controlled LC oscillators are injection-locked to provide quadrature outputs [44]-[45]. Though the Quadrature Voltage Controlled Oscillator (QVCO) is known to have two modes of operation, one with a 90º phase lead and one with a 90º phase lag, a Trojan mode can be inserted into the QVCO to introduce a third mode of operation. In the Trojan mode,

the quadrature outputs disappear. There is also a shift in frequency in the Trojan mode from the two quadrature modes of operation. All the three circuits can be triggered to the Trojan mode by setting proper initial conditions and all three circuits will be classified as benchmark circuits. Different initial conditions will cause the circuits to converge to different modes of operation if multiple stationary operating modes exist. Even during the design and simulation phases, the circuits may only be observed to operate at the desired mode, but they transition to the Trojan state when the operating conditions change to values that are in the domain of attraction of the Trojan state or mode.

2.2.3.1 Analog Trojan in three stage coupled ring oscillator

A coupled injection-locked three stage ring oscillator [46] is shown in Figure 2-22. Depending upon how the devices are sized, several different dynamic modes of operation have been reported. For some device sizing, this circuit exhibits two stable equilibrium points and one oscillatory mode. For other device sizing, it exhibits two distinct oscillatory modes. Depending upon the initial conditions, it can be forced to operate in any one of these modes of operation.

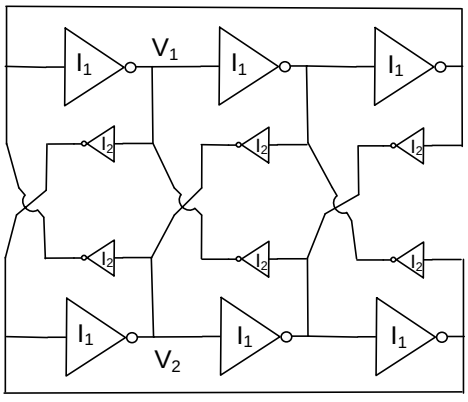


Figure 2-22 Three stage coupled ring oscillator

One implementation of the three-stage coupled ring oscillator circuit is shown in Figure 2-22. The inverters are all basic two-transistor CMOS circuits. An implementation of this circuit was made and simulated in a 0.5 μm ON CMOS process operating with supply voltages of VDD=2.5V and VSS=-2.5V. Minimum-dimension lengths were used for all devices. The n-channel devices in the I2 inverters were of minimum width. The p-channel devices in the I2 inverters had a width of 3 times that of the n-channel devices. The inverters denoted with I_1 were sized 6 times larger (i.e. the widths were increased by a factor of 6) than the inverters denoted with I_2. Transient simulation results for two different sets of initial conditions are shown in Figure 2-23. The initial conditions were set so that both modes of operation can be observed in the transient simulations.

The simulation results show that this circuit has two stationary oscillating modes which can be triggered by appropriately setting the initial conditions on the capacitors. In Mode 1, V1 and V2 are out of phase, whereas in Mode 2, V1 and V2 are in-phase. The two modes of oscillation have different oscillating frequencies and different peak-to-peak amplitudes. In Mode 1, the circuit's oscillating frequency is about 0.86GHz and peak-to-peak amplitude is 4V. However, in Mode 2, the circuit's oscillating frequency is about 0.4GHz with a peak to peak amplitude of 4.8V. If the oscillator is designed to obtain two 180^o out of phase signals, the in-phase mode would be a Trojan dynamic mode of operation, or vice versa.

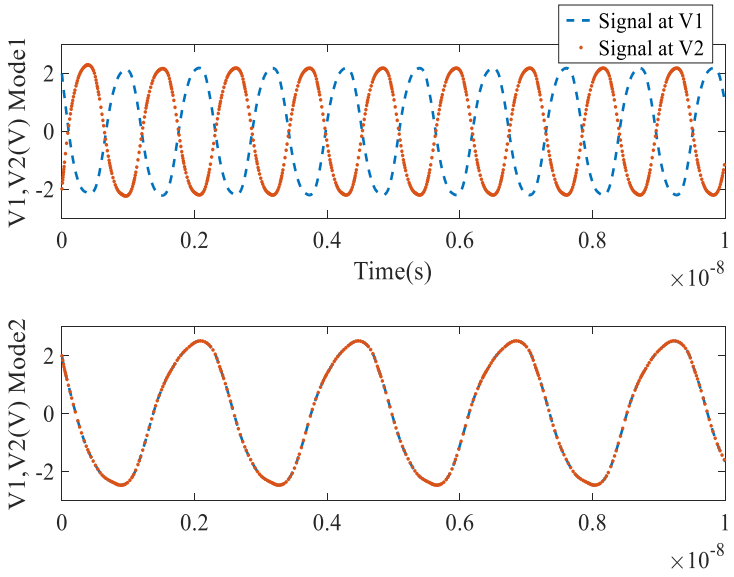
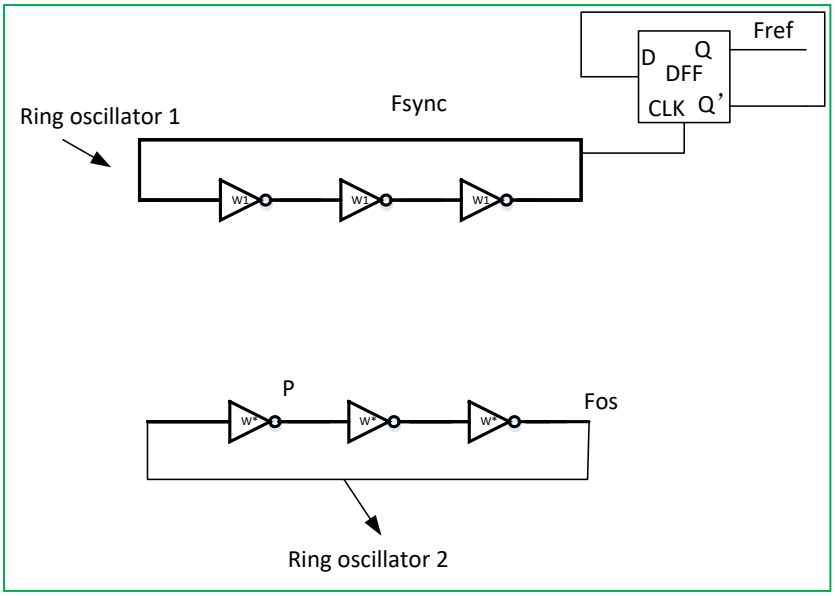


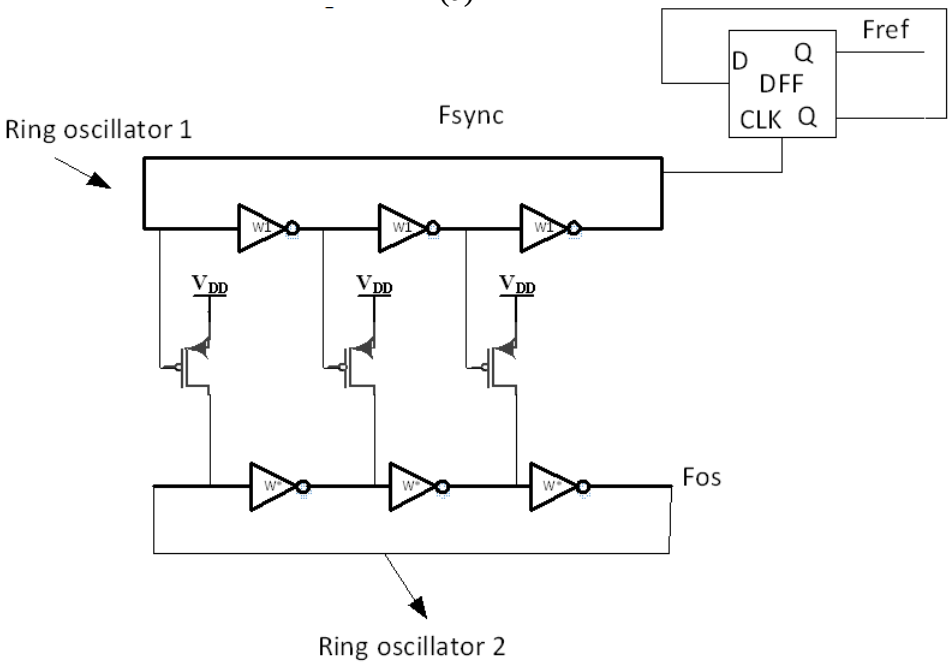
Figure 2-23 Simulation results for injection=locked ring oscillator of Figure 2-22 showing two modes of operation

2.2.3.2 Analog Trojan in injection locked frequency divider

Injection locking can be used to lock two oscillator circuits at the same frequency or lock one oscillator circuit to another oscillator's sub harmonic frequency. For systems with a frequency divider, injection locking in the circuits can have extra phase modes. The undesired phase relationship between signals can serve as Trojans in the circuit. The clock generator in Figure 2-24 can be used to generate these two signals which are operating at frequencies designated as 'Fos' and 'Fref'.

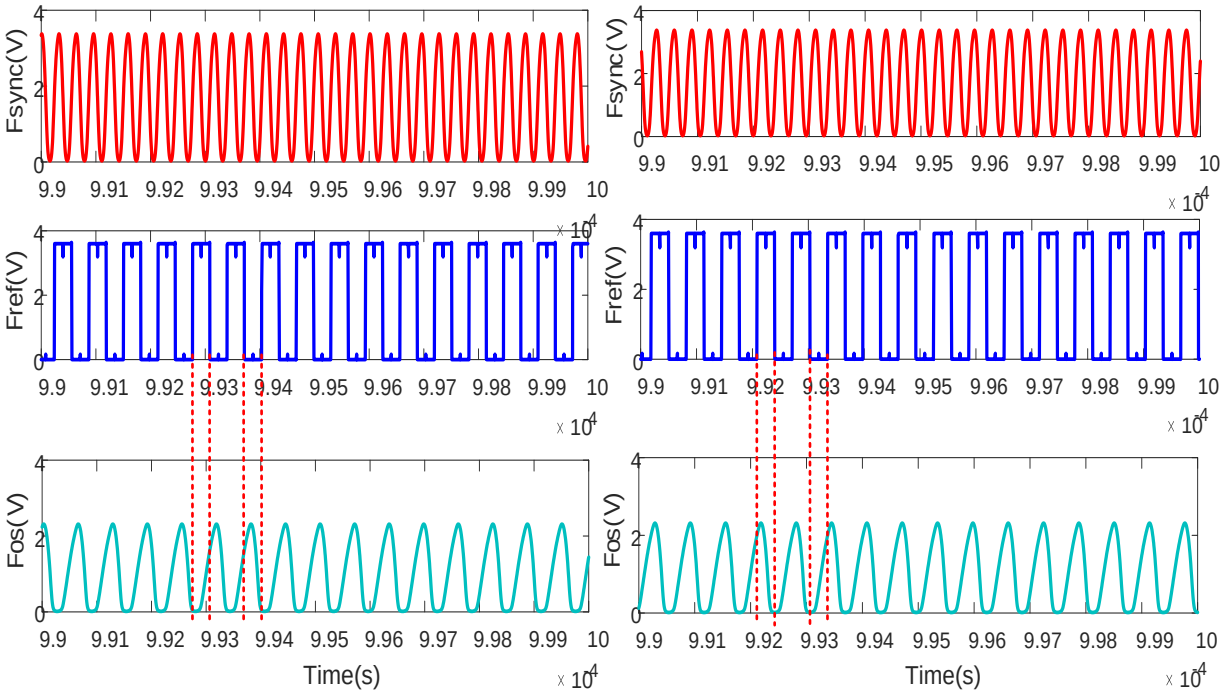


(a)



(b)

Figure 2-24 The configuration of frequency divider with extra mode existing; (a) Frequency divider and a separate ring oscillator; (b) Injection locked system



(a) (b)

Figure 2-25 Two modes in the circuit of Figure 2-24

In Figure 2-24 (a), there are two separate ring oscillator circuits. The signal generated by ring oscillator 1 has one oscillating frequency designated as ‘Fsync’, while the signal generated after the D-flip flop oscillates at a frequency designated as ‘Fsync/2’. The ring oscillator 2 generates signal oscillating around ‘Fsync/2’. In Figure 2-24(b), three transistors are used to sub harmonic injection lock these two ring oscillators. By doing injection locking, the oscillating frequency of ring oscillator 2 will be exactly half of the oscillating frequency of ring oscillator 1 and will be exactly the same as signal ‘Fref’. However, there are two possible phase relationships between the signals at node ‘Fos’ and the signal ‘Fref’ from the DFF.

The injection locking is implemented directionally with the three transistors from the top ring oscillator to the bottom ring oscillator, thus ring oscillator 2 is locked to the sub

harmonic frequency of the top oscillator. The frequency of the signal at 'Fos' will be exactly half of the oscillating frequency of ring oscillator 1. The signal at node 'Fos' will have the same oscillating frequency as the signal generated at DFF. However, it can be in phase or out of phase with the signal at node 'Fos' and the signal at 'Frev' with the phase determined by the initial conditions in both the upper and lower circuit. Simulation results for the injection locked oscillators designed in 0.5u ON process are shown in Figure 2-25. In the simulations, initial conditions were changed to excite the two different stationary modes of operation. In Figure 2-25 (a), the signal at 'Fref' and 'Fos' are out of phase, while in Figure 2-25 (b), the signal 'Fref' and 'Fos' are in phase. By implementing sub-harmonic injection locking, two signals can be locked to the same frequency but there may be one or more undesired phase relationships.

2.2.3.3 Analog Trojan in quadrature oscillators

The circuit shown in Figure 2-26 is a traditional quadrature LC oscillator. It is often used to generate 90° phase difference signals. The circuit has been designed with the device sizes given in Table 2-1 in an ON process with a supply voltage as 5V. It has been designed so that the phase difference between signals at nodes labeled Q1 and Q4 is 90° difference, which is the same as the phase difference between Q3 andQ2. However, because of the symmetrical characteristics, depending on the initial conditions, Q1 may be 90° leading Q4 or lagging Q4, and Q3 may be 90° leading Q2 or lagging Q2. These are the two modes of operation in this circuit which are well known. Simulation results showing the two modes of operation are shown in Figure 2-27. Depending on the initial conditions, the sequence of the four signals can be Q1, Q2, Q3, Q4 or Q1, Q4, Q3, Q2. If the phase sequence is critical in the system, the undesired mode is a Trojan mode.

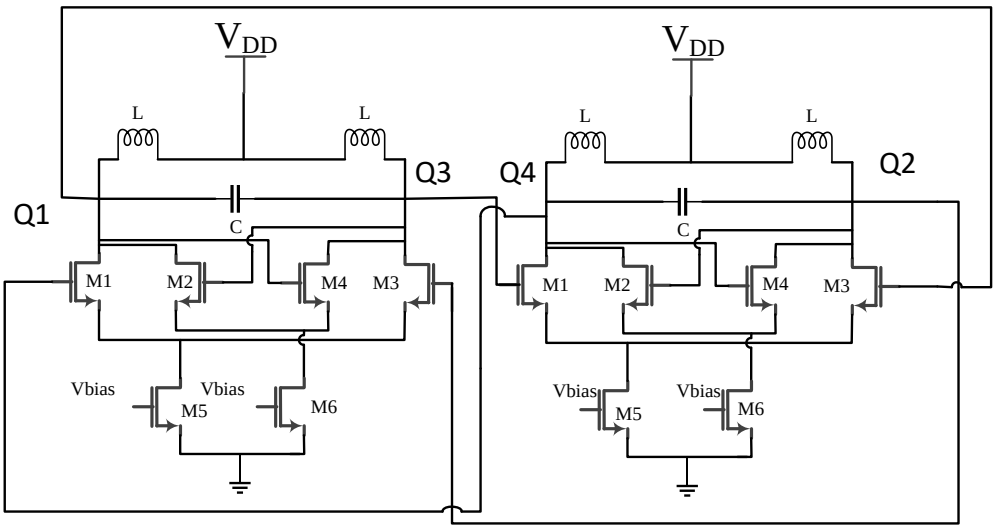


Figure 2-26 The conventional quadrature VCO

Table 2-1 size configuration of circuit in Figure 2-26

M1,M3	4(6u/1.2u)	L	1nH
M2,M4	5(6u/1.2u)	C	120pF
M5	8(6u/1.2u)	Vbias	1.2V
M6	10(6u/1.2u)		

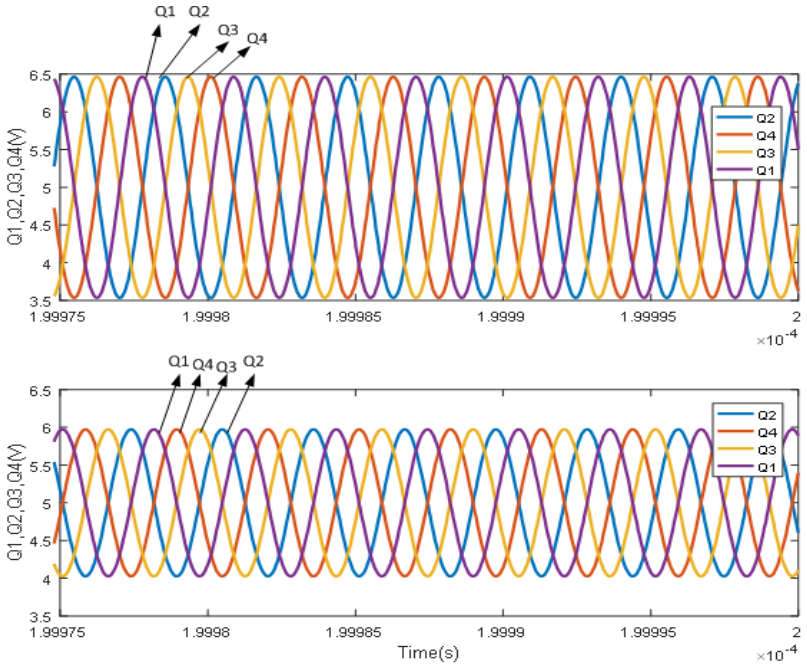


Figure 2-27 Two known modes in the conventional QVCO

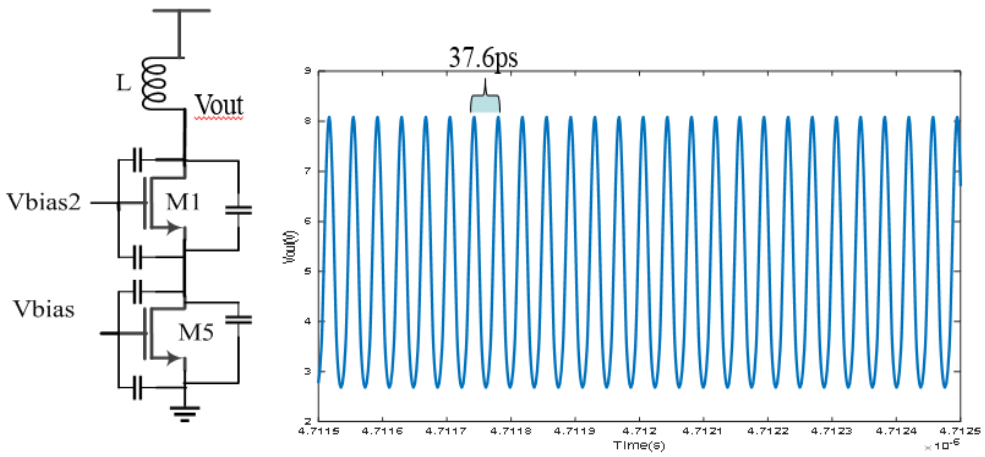


Figure 2-28 One signal path of the QVCO and its oscillating mode

The existence of the two modes of operation for this circuit has been reported in many papers. However, there is a third mode that can exist in this circuit as well with the same size configurations listed in Table 2-1 and this third mode has not been reported. This third mode is due to the presence of parasitic capacitors in the circuit. In Figure 2-28, one path of the quadrature oscillator that includes one inductor, the transistor in the middle, and the current source transistor is shown along with the parasitic capacitors. In this example, the biasing on the two gates has been set at 5V. This circuit can oscillate with proper initial conditions because of the parasitic capacitors. Simulation results of this circuit are shown in Figure 2-28. Since the parasitic capacitors are very small, the oscillating period is only 37.6ps.

The quadrature oscillator includes four paths of circuits shown in Figure 2-28. With the sizes in Table 2-1, and with the proper initial conditions, a third oscillating mode can be triggered and it is due to the parasitic capacitors. Simulation results for the quadrature oscillator showing the third mode of operation are shown in Figure 2-29. The oscillating frequency is hugely different from the two well-known modes of operation. The frequency of

the two known modes is about 350MHz whereas and the frequency of operation for the third mode is 12.5GHz. And, since the third mode of operation is dependent upon parasitic capacitances, the frequency of operation can be manipulated by an unscrupulous designer by layouts that may change the size of the parasitic capacitances.

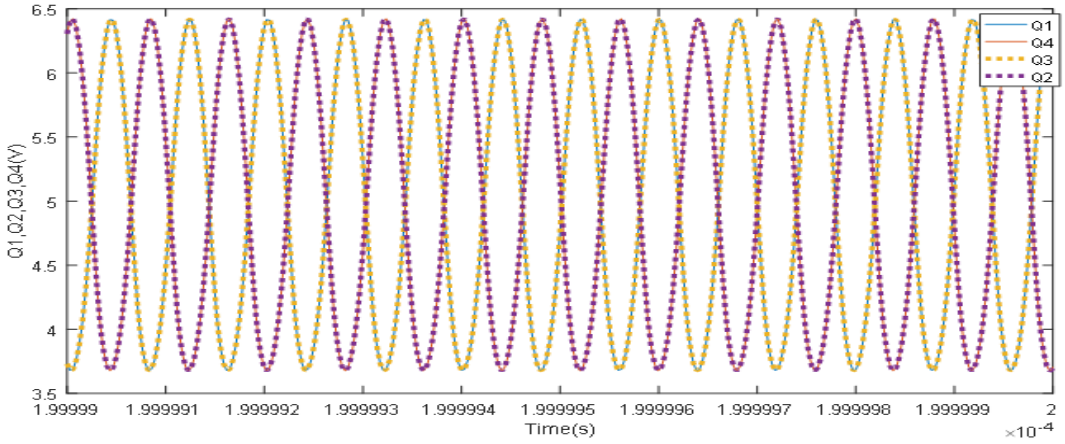


Figure 2-29 The third mode in the QVCO with sizes in Table 2-1

If this circuit is designed and used, the extra two modes (the undesired phase or the undesired high frequency of oscillation) are PAAST Trojans and disastrous results can happen because of the phase and frequency differences.

Once vulnerability to the presence of the third mode of operation is recognized, methods can be established to eliminate it. Though not the focus of this research, it can be shown that if the loop gain of the positive feedback loop is large enough, the third mode can be eliminated.

2.3 Comparison with a kind of PAAST Trojans in digital circuits

As shown in the examples, the Trojans in analog circuit can be in amplitude voltage domain, frequency domain, or phase domain. If the Trojan is triggered, important data can leak or the system may be denial of service because of the undesired frequency, phase or amplitude. Especially in military, medical treatment area, the results brought by these

Trojans can be catastrophic. These analog hardware Trojans served by extra operating points or modes can easily be inserted into many commonly used circuits. The existence of this type of Trojan requires no additional circuitry, no increase in power, no increase in area, no changes in architecture, and that leave no signatures in either power or timing busses prior to triggering. The PAAST characteristics make the Trojan hard to detect.

A kind of hardware Trojan which can be embedded in arbitrary finite state machine is discussed in [47] and these kinds of Trojans are also with PAAST characteristics.

The Trojan described in [47] is the redundant state or 'don't care states' in the state machine. A state machine as an example is shown in Figure 2-30. It has three normal working states '00' '01' '10', and one redundant state '11'. The state machine can have transitions from one of these three states to another working state. Normally, there is zero probability for transitions happening from any of the three working state to the redundant state. However, if there is some trigger mechanism added, it can trigger the state machine to work at this redundant state or make the redundant state occur during the normal transition time. Since the redundant state inherently exist in the state machine, a Trojan served by this redundant state will also have no power, architecture, area overhead or with any signature variation. Thus, as Trojans, the redundant state in state machine has the same property as the extra equilibrium state/mode in analog circuit.

However, different to the PAAST Trojans served by extra operating points or modes in analog circuit of which the existence is not known, the existence of the redundant state in the state machine is already known by the designer. It only needs to detect whether the circuit has any potential trigger mechanism inserted into the circuit to make the transition to the redundant state happen. But for the Trojan in analog circuit, it is not only necessary to detect

the trigger mechanism but also need to detect the presence of the extra equilibrium states. Comparing to the PAAST Trojan in digital circuits, the analog PAAST Trojan is even more challenging and difficult to detect.

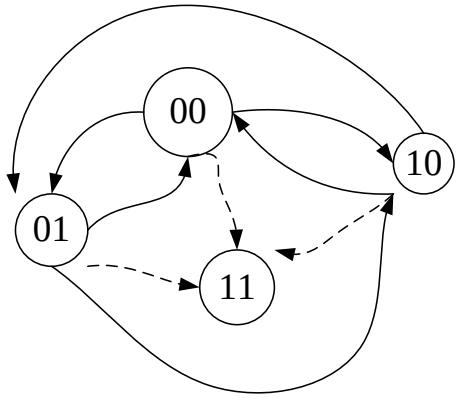


Figure 2-30 State machine with 3 normal states and 1 redundant state

2.4 Temperature signatures in analog static circuit

2.4.1 Three temperature signatures observed in Inverse Widlar circuit

Three different implementations of the inverse wilder circuit are shown in Figure 2-31 designed in a 0.5u ON CMOS process, are characterized by the device sizes (W and L values along with multiplier factor) shown in Table 2-2. These three implementations are designated as Type 1, Type 2, and Type 3 circuits, showing three different temperature signatures of multiple equilibriums in this circuit. The inverse Widlar circuit exclusive of a start-up circuit in Figure 2-31 can be used as a bias voltage generator, a bias current generator or a temperature sensor, as reported.

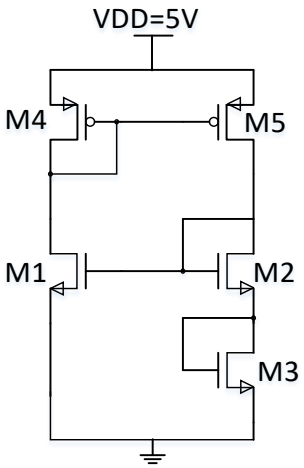


Figure 2-31 Inverse Widlar circuit

Table 2-2 Three types of example circuits' sizes

Sizes and types	Type 1	Type 2	Type 3
M1(W/L)*M	(1.5u/3u)*1	(1.5u/3u)*1	(1.5u/3u)*1
M2(W/L)*M	(4.8u/600n)*1	(1.5u/900n)	(1.8u/600n)*10
M3(W/L)*M	(2.4u/600n)*1	(2.4u/600n)*1	(1.5u/600n)*1
M4(W/L)*M	(3u/3u)*5	(3u/3u)*5	(3u/3u)*5
M5(W/L)*M	(3u/3u)*5	(3u/3u)*5	(3u/3u)*5

2.4.1.1 Type 1 signature-one operating point in temperature domain

Type1 signature: Simulation results for the Type 1 implementation are shown Figure 2-32. With this implementation, no hysteresis window is observed and the circuit has a unique solution at each temperature. This operation has been confirmed by doing a break-loop homotopy analysis like that described in [48] at a large number of individual temperature values. If this unique solution signature is maintained over process and supply voltage variations, a start-up circuit is not needed for this implementation.

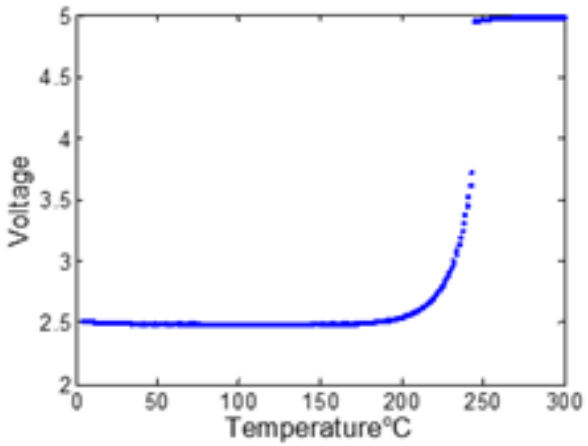


Figure 2-32 Type 1 signature: single operating point in each temperature

2.4.1.2 Type 2 signature-Hysteresis window in the temperature domain

Type2 signature: Simulation results for the Type 2 circuit showed a hysteresis window where the discontinuities which define the edges of the hysteresis window occurred at 52°C and 183°C. The actual temperature characteristics which have a continuous transition between a single operating point and multiple equilibrium points are shown in Figure 2-33. This is designated as a Type 2 signature. This implementation has three equilibrium points for $52^{o}C < T < 183^{o}C$. If the intended operation of this circuit is as a voltage reference, current reference, or temperature sensor, a start-up circuit is needed to eliminate the undesired stable equilibrium point.

Both the location and the width of the hysteresis window can be changed by adjusting the sizes of some transistors. Thus, instead of using a start-up circuit to eliminate the undesired equilibrium point the circuit can be used as a temperature trigger circuit [49] by programming one edge of the hysteresis window of circuits with a Type 2 signature so that it occurs at the desired trigger temperature. A detailed design of temperature trigger circuit is discussed in the following section.

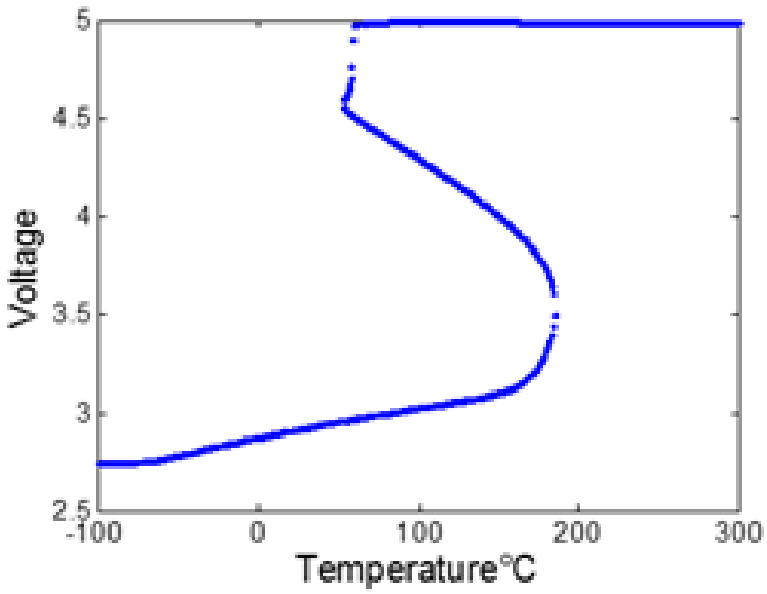


Figure 2-33 Type 2 signature - continuous transition between single and multiple operating points

2.4.1.3 Type 3 signature- isolation region in the temperature domain

Type3 signature: Simulation results for the Type 3 circuit are shown in Figure 2-34. This signature is characterized by a part of the temperature characteristics that cannot be reached by a continuous perturbation from some other parts of the temperature characteristics. The locus of points that form a closed curve will be termed an isolation region. A Type 3 signature is characterized by an isolation region. This Type 3 circuit has three equilibrium points for $3^{o}C < T < 118^{o}C$. If designed to operate at a single equilibrium point, a start-up circuit would also be required to eliminate the isolation region. The presence of multiple equilibrium points when an isolation region exists cannot be easily detected with a bi-directional temperature sweep (discussed in Chapter 3).

The location and size of the isolation region can also be controlled with judicious device sizing. With the device sizes shown in Table 2-3, the very narrow isolation region shown in Figure 2-35 is obtained. Circuits with narrow isolation regions may also be very

difficult to verify with standard homotopy methods since the multiple equilibrium points would not be present if the simulation temperatures were outside of the narrow range corresponding to the isolation region.

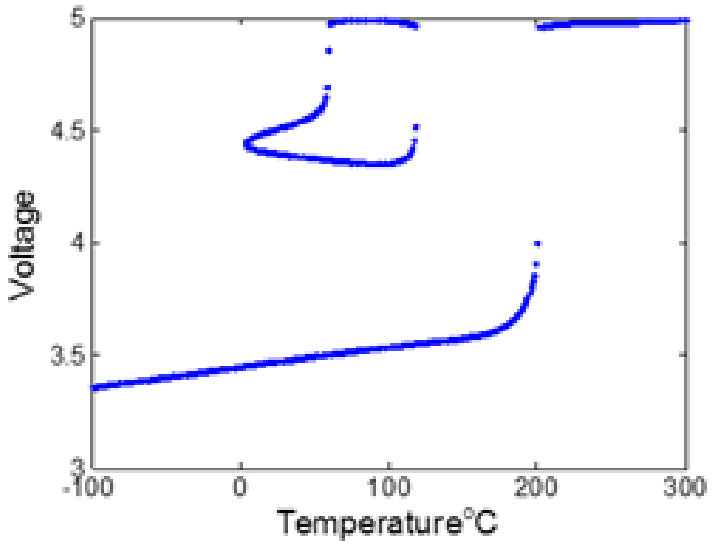


Figure 2-34 Type 3- an isolated region in a temperature range

Table 2-3 sizes of example circuit with very narrow isolated region

M1	M2	M3	M4	M5
(1.5u/3u)*1	(2.1u/600n)*1	(2.4u/600n)*1	(3u/3u)*5	(3u/3u)*5

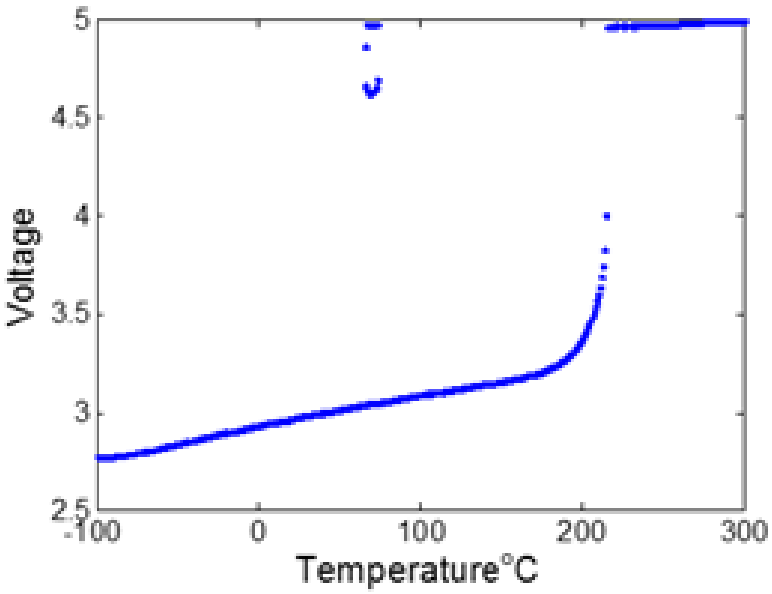


Figure 2-35 Operating points with a narrow isolated region in a temperature range

Though the three identified signatures were presented as examples with the inverse Widlar structure of Figure 2-31, it can be shown that these signatures can also exist in other widely used circuits.

2.4.2 Temperature trigger design based on Schmitt trigger circuit

As discussed in previous sections, multiple equilibrium points are sensitive to temperature variations. In most condition, the extra operating point in static analog circuit is undesired and termed as Trojans. However, designers may also explore the characteristics of circuits with multiple equilibriums for some specific and practical use. In this section, a temperature trigger circuit is designed by exploring a type 2 temperature signature in a Schmitt trigger circuit.

In many high-performance applications, local power densities are increasing with decreasing feature sizes in newer CMOS process. The increasing power densities often cause a localized increase in temperature or an increase in temperature across the die. High

temperatures invariably influence the performance of a circuit, cause the circuit to fail, and/or degrade the lifetime of IC. To mitigate these concerns, localized on-chip thermal monitoring circuits have become an integral part of the power/thermal management of the integrated circuit. In most power management approaches, the system is protected [50] by frequency throttling, task reassignment, or thermal shutdown whenever the temperature exceeds a predetermined trigger temperature.

Most of the existing temperature sensor or thermal monitoring circuits are based on the temperature dependence of some characteristics of the devices that are available in a given process. Two properties of devices available in CMOS processes are often discussed in the literature for building on-chip temperature sensors. One is the thermal voltage and another is the threshold voltage. References [51][52] present temperature sensor circuits that use the temperature dependence of the threshold voltage and the thermal voltage respectively to build temperature sensors.

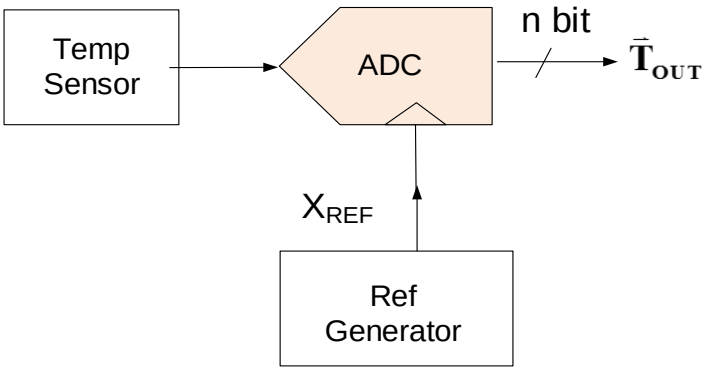


Figure 2-36 The standard temperature monitoring (temperature to digital) system

A standard temperature monitoring system that provides a digital representation of the temperature is shown in Figure 2-36 [53]. The three core parts of the system are the temperature sensor, a reference generator circuit, and an ADC module. In a power

management system, the output code is typically read periodically from the A/D module and compared with the predetermined trigger temperature. Based upon this comparison, action is initiated if necessary to guarantee the temperature remains below the critical temperature. Due to delays associated with temperature measurement, corrective action, and thermal propagation, hysteresis in the temperature is often observed [54].

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 point [48]. Start-up circuits require a modest increase in area and it may be difficult to verify that they are effective over local and global PVT variations.

A low power and ultra-small temperature trigger circuit is introduced in section based on the multiple equilibrium in the circuit. It is based upon a Schmitt trigger structure with only four transistors required to generate a programmable hysteresis window in the temperature domain. The Schmitt trigger circuit is generally viewed as a circuit that exhibits a hysteresis window in the input voltage / output voltage plane obtained by sweeping the input voltage forward and backward. More precisely, it is characterized by a region of input voltages that have more than one output voltage. The hysteresis window is attributable to the presence of a positive feedback loop.

In contrast to a conventional Schmitt trigger circuits where the input variable is a voltage, in a temperature trigger circuit the input variable is temperature and the output variable is a Boolean variable. But like the conventional Schmitt trigger circuits, a temperature trigger circuit with hysteresis is characterized by a region of input temperatures

that have more than one output voltage. With appropriate simulators, the hysteresis can be exhibited by sweeping the input temperature forward and backwards. The temperature trigger circuit introduced here will exhibit hysteresis when the input temperature is swept forward and backwards using the SPECTRE simulator. For power management, hysteresis window in temperature domain will help to avoid frequently turning off or turning on of responded circuits.

2.4.2.1 Threshold voltage based temperature trigger with hysteresis

A Schmitt trigger circuit is shown in Figure 2-37 [55]. With the parameters K_p and β defined by the expressions

$$K_p = \frac{(W_{p1}/L_{p1})}{(W_{p2}/L_{p2})}, \beta = \frac{\mu_{COX} W}{L} \tag{2-5}$$

It was shown that the boundaries of the hysteresis region in the V_{OUT}: V_{IN} plane are given by the expressions

$$V_{T+} = \frac{V_{DD} + V_{Tp} + \sqrt{\frac{2\beta_n}{\beta_p}} V_{Tn}}{1 + \sqrt{\frac{2\beta_n}{\beta_p}}} \tag{2-6}$$

$$V_{T-} = \frac{V_{DD} + V_{Tp} + \sqrt{\frac{2\beta_n}{\beta_p}} V_{Tn}}{1 + \sqrt{\frac{2\beta_n}{\beta_p}}} - \frac{V_{DD} + V_{Tp}}{(1 + \sqrt{\frac{2\beta_n}{\beta_p}})(1 + \sqrt{K_p})} \tag{2-7}$$

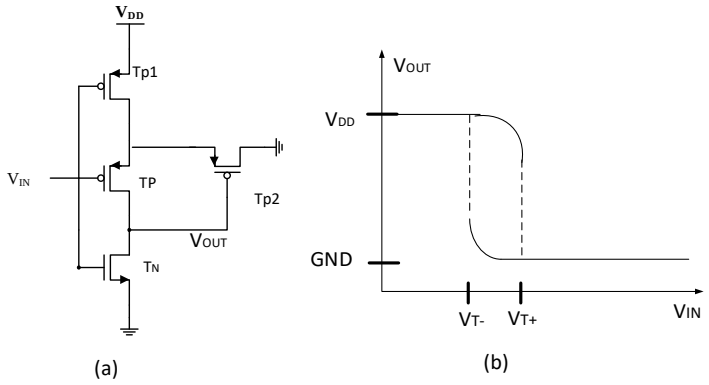


Figure 2-37 Schmitt trigger circuit and return map

The hysteresis region at a fixed temperature is apparent in the bi-directional input sweep shown in Figure 2-37 (b). From Equation (2-6) and (2-7), it is apparent that both the location and the width of the hysteresis region are dependent upon both design parameters and the threshold voltage.

The threshold voltage is temperature dependent. In the BSIM model, this temperature dependence is modeled by the expression

$$V_{th}(\mathrm{T}) = \mathrm{V}_{th}(\mathrm{TNOM}) + (\mathrm{KT1} + \frac{\mathrm{KT1L}}{L_{eff}} + \mathrm{KT2} \bullet V_{bseff})(\frac{T}{TNOM} - 1) \qquad (2\text{-}8)$$

Neglecting the effects of V_{bseff}, it follows Equation (2-11) that the threshold voltage is linearly dependent on temperature and can be expressed as

$$V_{th} = k \times T + VTH0 \qquad (2\text{-}9)$$

Where the parameter k is the slope and VTH0 is the 0 K axis intercept. A typical value of k for n-channel MOSFETs is around -1.32mV/oC. It thus follows that V_{T+} and V_{T-} in (2-6) and (2-7) are both approximately linearly dependent on temperature. Thus, for an appropriate fixed input voltage V_{IN} and appropriate device sizes, V_{T+} and V_{T-} will be equal to V_{IN} at different temperatures. It follows that this circuit can be designed to have a hysteresis

window in the temperature domain. If a comparator is connected to the output of this Schmitt trigger circuit, the relationship between the comparator output and the input temperature will be a two-level output with hysteresis. The temperature trigger circuit is shown in Figure 2-38 (a). The fixed input to the Schmitt trigger block, denoted as the "Thermal Hysteresis Block", is the dc voltage V_{BB}. The comparator is implemented with a basic CMOS inverter. The transfer characteristics of the temperature trigger circuit showing the hysteresis in the temperature domain are shown in Figure 2-38 (b).

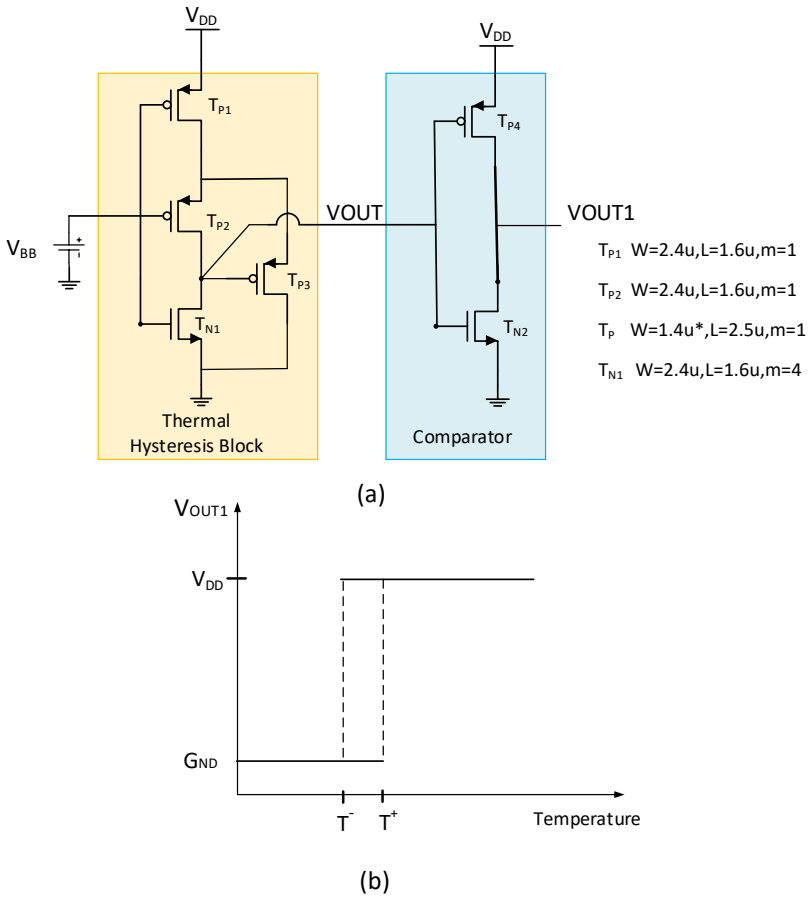


Figure 2-38 Temperature trigger (a) proposed circuit (b) output voltage vs temperature

For a fixed input voltage, if we neglect the temperature dependency of VTP, it follows from (2-6) and (2-7) that V_{T+} and V_{T-} also have linear relationships with temperature with identical slopes but with different offsets that can be expressed as

$$V_{T+} = a \times T + m \tag{2-10}$$

$$V_{T-} = a \times T + n \tag{2-11}$$

Where the parameters α, m, and n can be obtained from (2-6) and (2-7). These linear functions are depicted in Figure 2-39 (a).

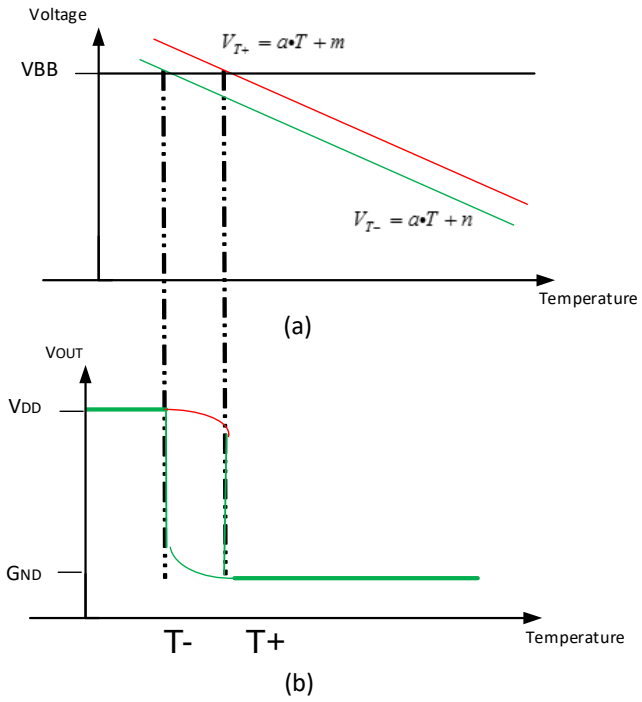


Figure 2-39 Hysteresis window in temperature domain

When the input voltage is fixed at V_{BB}, it will intersect with the V_{T+} and V_{T-} lines at the two distinct temperatures T+ and T-. These two temperatures form the boundaries of a hysteresis window for V_{OUT} in the temperature domain as shown in Figure 2-39(b). For different input voltages, the two intersections with the V_{T+} and V_{T-} lines occur at different temperatures but the center of the hysteresis region moves almost linearly with the input

voltage. But the difference between T+ and T- for different values of V_{BB} are constant when the lines for V_{T-} and V_{T+} are parallel. In this way, the location of the hysteresis window can be varied by changing the input voltage while keeping the width of the hysteresis window fixed as shown in Figure 2-40.

The difference between V_{T+} and V_{T-} , designated as V_H, is given in Equation (2-12).

$$V_H = \frac{V_{DD} + V_{Tp}}{(1+\sqrt{\frac{2\beta_n}{\beta_p}})(1+\sqrt{K_p})} \tag{2-12}$$

It follows that the width of the hysteresis window in the temperature domain is given by

$$(T+)-(T-) = \left|\frac{V_H}{a}\right| \tag{2-13}$$

Though the hysteresis window width is fixed for a given value of VH, the width can be changed by changing the design variables β_n, β_p, or K_P.

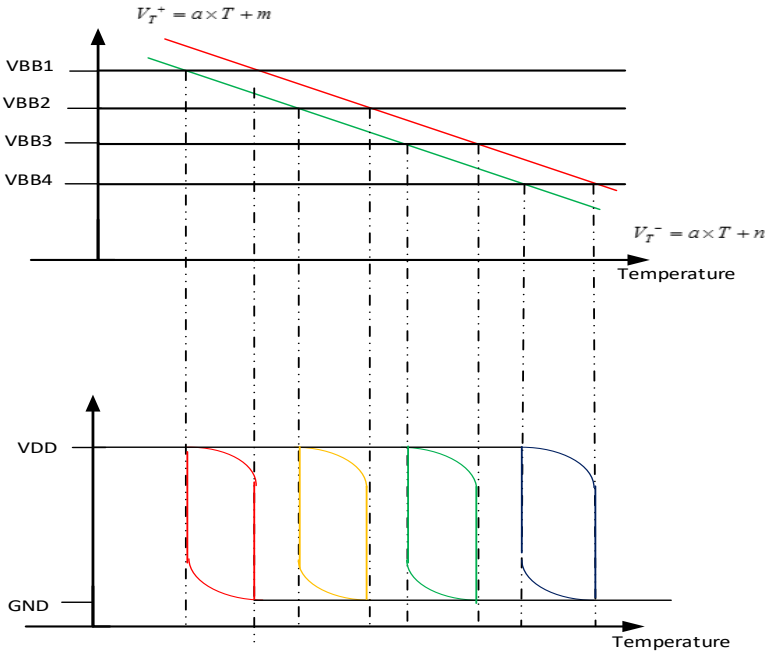


Figure 2-40 Hysteresis window's location variation

The equal slope of the V_{T+} and V_{T-} lines is attributable to the assumption that the temperature dependence of V_{Tp} could be neglected. If the temperature dependence of V_{Tp} is included, the locus of V_{T+} and V_{T-} will still be nearly linear but the slopes will be different as depicted in Figure 2-41. This will cause a modest change in the width of the hysteresis window in the temperature domain if the input voltage is changed to move the hysteresis window along the temperature axis and introduce a small nonlinearity in the relationship between the input voltage and the center of the hysteresis window.

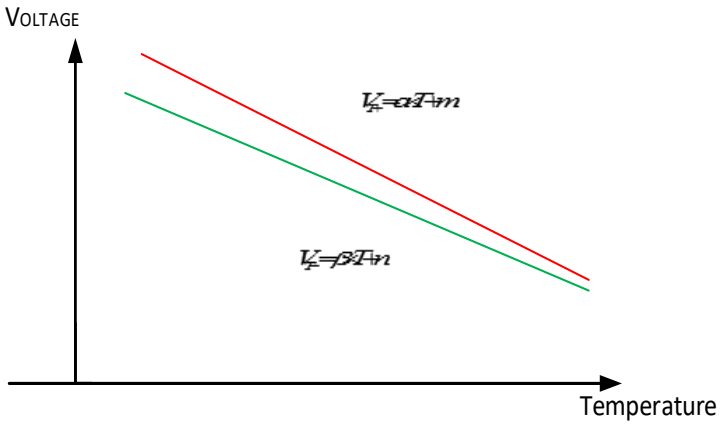


Figure 2-41 V_{T+} and V_{T-} with diffident temperature coefficients

The effects of including the temperature dependence of the threshold voltage of the p-channel devices on the movement of the hysteresis window with the input voltage is shown with a SPECTRE simulation of one implementation of this circuit in Figure 2-42. It is apparent that in this design that the change in the width of the hysteresis window as it is moved along the temperature axis with changes in the input voltage is modest. Also, this small 'Δlocation ' variation can be compensated by the control circuit in Figure 2-43 (a) with temperature characteristics in Figure 2-43 (b).

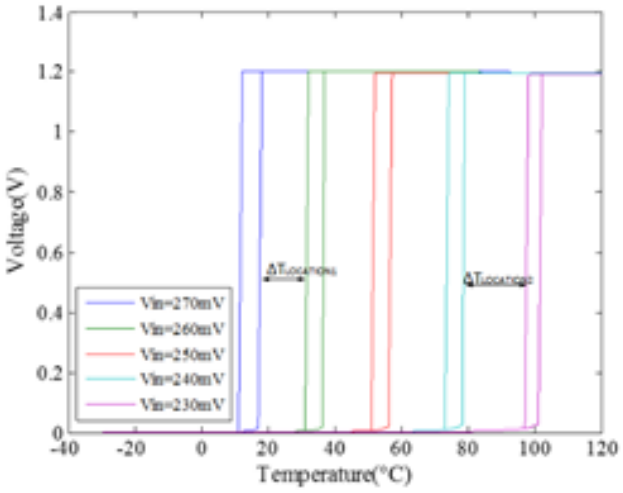


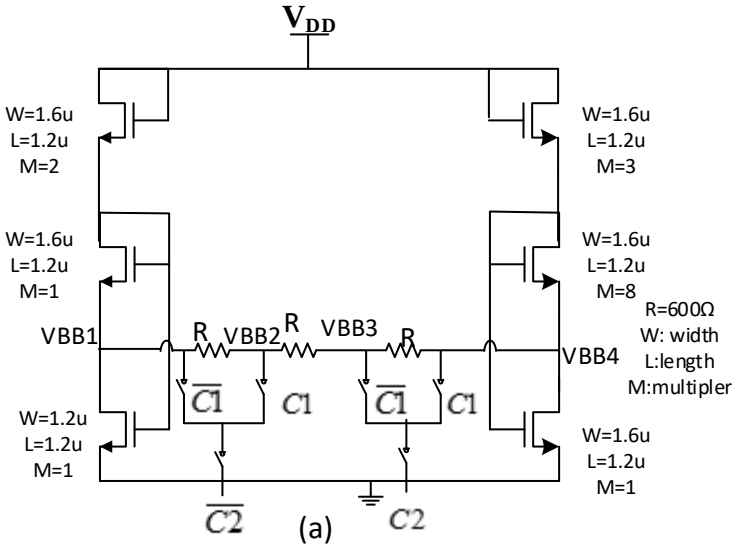
Figure 2-42 Simulation results at different input voltage

2.4.2.2 Programmable circuit

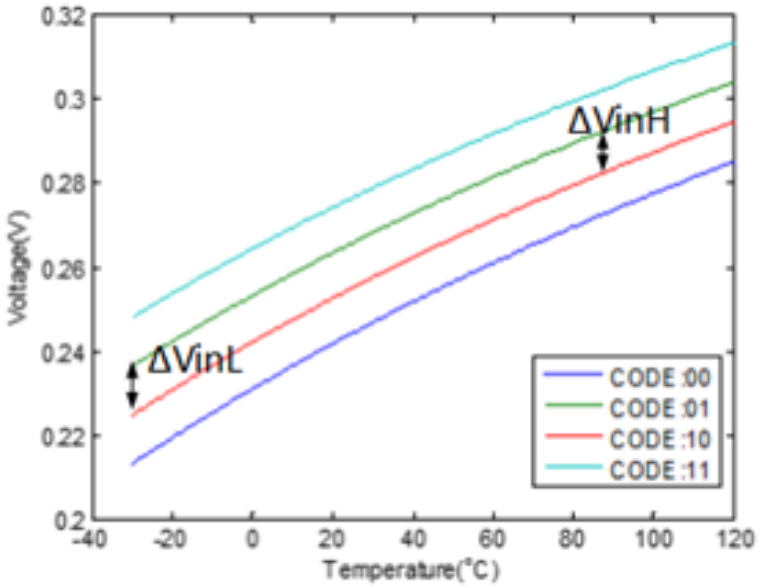
The location of the hysteresis window can be made programmable by adjusting the input voltage V_{BB}. One simple circuit that can be used to adjust the input voltage is shown in Figure 2-43. In this circuit, the switches which can be controlled by a digital MUX are made of single MOS transistors and the devices on the left and right sides of the circuit are sized to create a small voltage gradient in the voltages at the intermediate nodes of the resistor string.

This hysteresis location circuit was combined with the temperature trigger of Figure 2-38 to provide a programmable temperature trigger with a 2-bit window location control. This programmable temperature trigger circuit was designed in a 0.13µm CMOS process with poly silicon resistors used for the resistor string. The circuit was biased with a single 1.2V supply. Device sizes in this design are given in the circuit figure. SPECTRE simulation results of the temperature trigger are shown in Figure 2-43 (c). It can be seen from these simulation results that the hysteresis window is programmable over a reasonably large range and that the width of the hysteresis window does not change significantly with position. Finer resolution can be easily obtained with minimal area overhead if needed in a specific

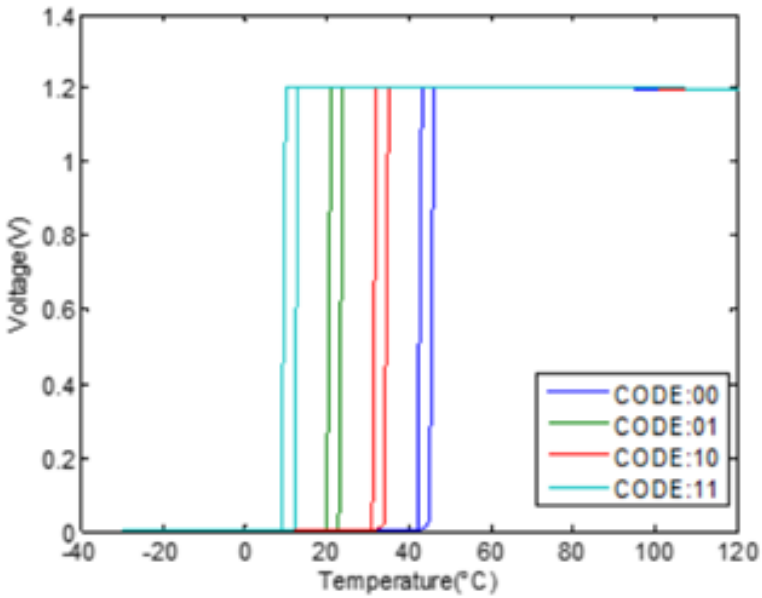
application. And, if tighter control of the width of the hysteresis window is needed, the width can be programmed by digitally adjusting β_n, β_p, or K_P. In most power management applications, this adjustment would likely not be necessary.



(a)



(b)



(c)

Figure 2-43 Input voltage control circuit and simulation results

A very small programmable temperature trigger circuit with hysteresis suitable for power management applications has been introduced by exploring the type 2 temperature signature of multiple equilibriums in a Schmitt trigger circuit. Both the location and width of the hysteresis window can be digitally programmed. When designed in a 0.13um process, the total power dissipation of the programmable temperature trigger is 72μW, and the total area is 25um×30um.

CHAPTER 3. DETECTION METHOD OF PAAST TROJANS IN ANALOG CIRCUITS

PAAST analog hardware Trojans can make the circuit have performance alteration, resulting to malfunction or information leakage. However, since the extra operating points/modes inserted in the circuit are because of the circuit structure and devices' sizes configuration, there is no any physical characteristics variation compared to the Trojan free circuit, such as any power, area overhead, circuit architecture difference, signature variation in the power supply bus, or delay changes in the timing path, which makes it very difficult to detect. Almost all the existing Trojan detection methods [56]-[58], are normally based on the difference of these physical characteristics compared to the Trojan free circuit to detect the presence of Trojans. Because of the transparent characteristic of this type of Trojans, all these existing methods would fail to detect the presence of the Trojan served by the undesired operating points. Even the circuit is given with details of topology, it is still very hard to verify the circuit, specifically when the circuit is large and complex. However, since many analog circuits are designed with positive feedback loops, this type of Trojans is easily to be inserted to even very commonly used analog circuits.

In this chapter, methods detecting PAAST hardware Trojans in analog static circuit and dynamic circuit will be introduced.

3.1 Methods to detect PAAST hardware Trojans in static analog circuits

3.1.1 State of art of method to detect multiple equilibrium points

Identifying the presence of an undesired stable equilibrium point with a simulator is complicated by the fact that such points may exist only over a portion of the process, voltage, and temperature (PVT) domain. Correspondingly, verifying the effectiveness of start-up circuits is complicated by the same issues. The problem is more challenging because circuit

simulators only provide a single output at any point in the PVT domain even when multiple outputs exist irrespective of whether the designer is or is not aware of the presence of undesired stable equilibrium points in the circuit. But the biggest challenge is more fundamental in nature. The problem of finding all solutions of a set of nonlinear equations remains an open problem in the mathematics and computer science research communities and it remains unknown whether all stable equilibrium points in even some basic circuits are recognized by the designers. If an undesired stable equilibrium point remains undetected, a circuit is vulnerable to failure if it enters this undesired state. Thus, methods of identifying undesired stable equilibrium points, even if they cannot guarantee all operating points have been identified, are of use [24][59]-[64]. Homotopy methods are often used to identify multiple equilibrium points though in the general case even these methods will not necessarily find all equilibrium points.

3.1.1.1 facts and anti-facts of simulators

Circuit simulators are specifically designed to solve the set of linear and nonlinear equations that characterize the operation of a circuit and they do this very well. For this reason, it is highly desirable to use circuit simulators to address the multiple equilibrium point challenge. In simulators such as Spectre, homotopy methods are used to trace the DC solutions. However, in this application, they are structured to just find one solution and then stop. Since circuit simulators provide only a single solution for an output voltage or output current, simulation strategies need to be developed that may help identify the presence of multiple equilibrium points. In Cadence's parametric analysis simulation method, it does not couple simulation results from one temperature step to the next in a temperature "sweep" so the simulation results obtained from stepping temperature are all independent from each got at different temperature. But it will be shown by example that the lack of coupling in

temperature “sweeps” may be beneficial in some situations for determining the presence of multiple equilibrium points since the coupling between simulation steps has been severed.

The widely-used Wilson bias generator, without a start-up circuit, is shown in Figure 3-1. The simulation is based on 0.5u ON process. The circuit has been designed so that the desired operating point is close to 3.5V over the temperature range from 0°C to 120°C. A parametric analysis sweeping method in temperature domain for an implementation of this circuit was made in Spectre and the results, which show a single output for each temperature point, are shown in Figure 3-2 (a). These somewhat peculiar results may appear to raise questions about the simulation. Removing the interconnection points which are an artifact of the graphing routine used to display the output data, the actual simulation data shown in Figure 3-2(b) is obtained. As will be discussed in the following section, this simulation provides very useful information about the circuit and not only shows the presence of more than one stable equilibrium point at temperatures above 65°C; it also shows the presence of an unstable equilibrium point.

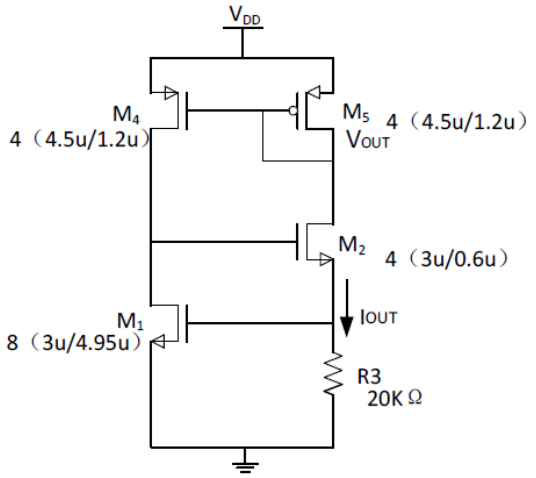


Figure 3-1 Wilson circuit

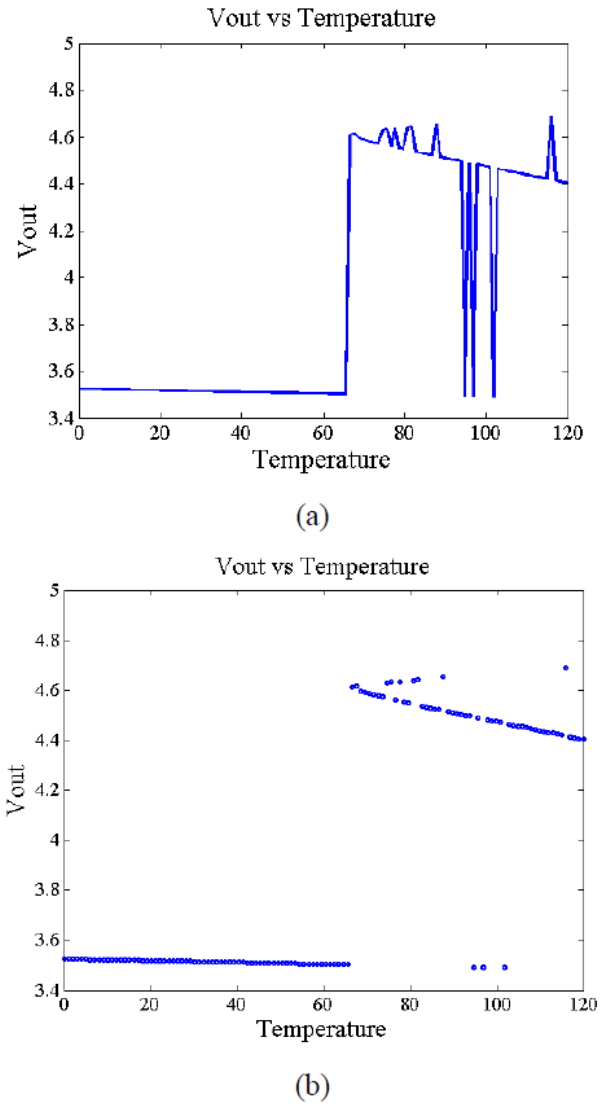


Figure 3-2 Simulation results of parametric analysis of temperature

However, the success demonstrated in the simulation shown Figure 3-2 for identifying the presence of more than one equilibrium point is not predictable. Consider a second example that has two Wilson bias generators in one circuit schematic as shown in Figure 3-3 (a) where all that the two circuits share in common is the ground node. The corresponding graphical representation of this circuit is a “hinged-graph”. The circuits are identical except for a start-up circuit which has been added to the circuit on the right. Simulation results of a temperature sweep are shown in Figure 3-3(b). The two outputs show

an identical dependence on temperature and do not show any evidence of the three equilibrium points that exist for the circuit on the left at temperatures above 65°C which were shown when the circuit was simulated by itself. Other combinations of circuits into a schematic with a hinged graph have also shown differences between the results obtained with a combined simulation and those obtained with individual simulations. Numerical coupling in the simulator affects the simulation results of circuits with multiple equilibrium points.

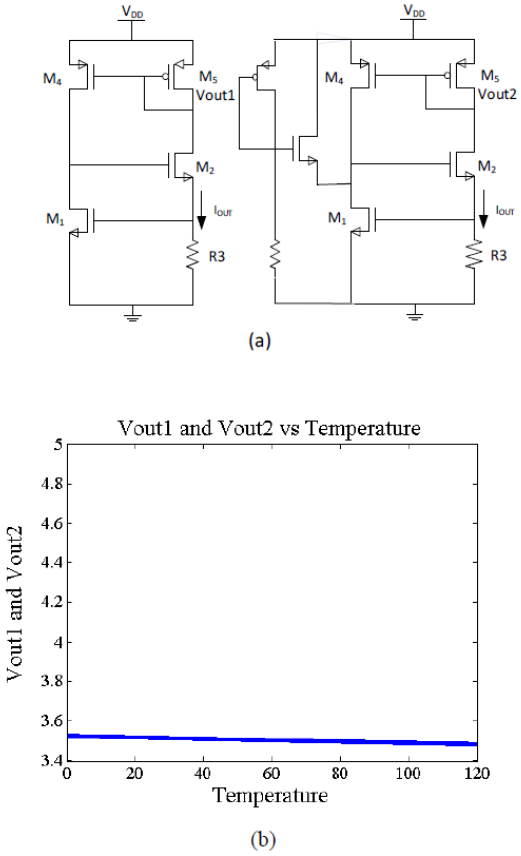


Figure 3-3 The anti-facts of simulators when simulating two circuits

Consider again the simulation results shown in Figure 3-2 (b). There are corresponding operating points for the other two intermediate node voltages in the circuit. Every point in the figure is one solution but it may not be the only one. From the simulation results, three trend lines or trend traces can be seen. So based on these results, different initial

voltages can be set on all internal nodes prior to doing the parametric analysis in temperature domain. The initial voltages will serve as a point of attraction for the solutions. Figure 3-4 shows simulation results obtained by sweeping temperature with different node sets close to those determined from the simulation results of Figure 3-2(b). Simulation results for setting an initial condition on the V_{OUT} node of 3.3V are shown in Figure 3-4(a). Figure 3-4(b) shows the results when the output node is set at 4.2V. Figure 3-4 (c) shows simulation results when the output node is set at 4.6V. The results are combined to obtain the transfer characteristics shown in Figure 3-4 (d). From Figure 3-4(d), it can be seen that the circuit has three equilibrium points when the temperature is larger than 65°C but a single operating point at temperatures below 65°C. Note that the results in Figure 3-2(b) obtained with a single sweep is consistent with the transfer characteristics shown in Figure 3-4(d) but from an interpretation of the results of Figure 3-2(b), the multiple equilibrium points were predicted.

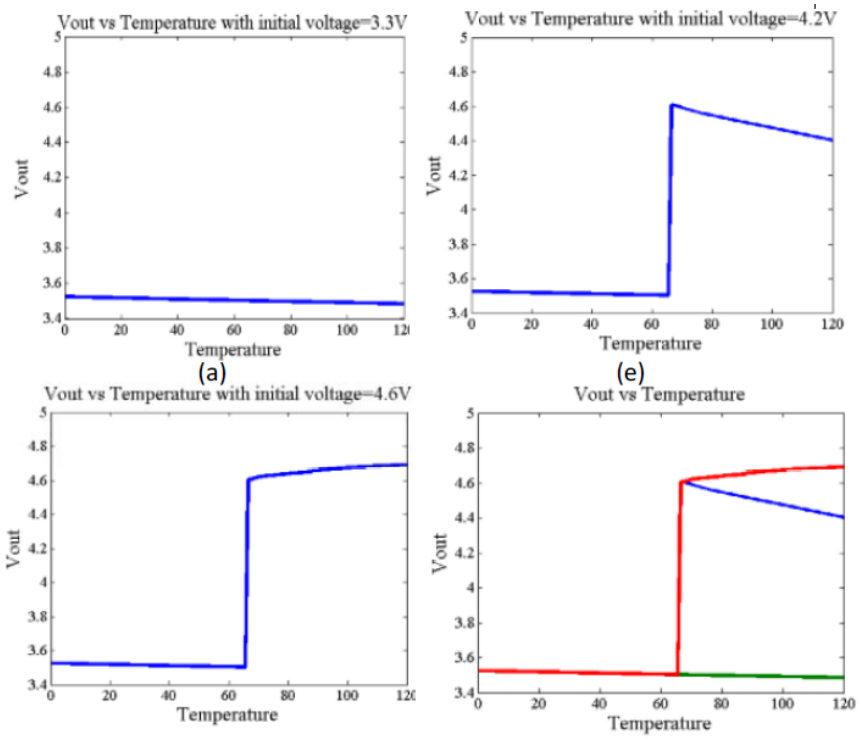


Figure 3-4 Simulation results with different initial condition voltage

3.1.1.2 Existing methods to detect Trojans in analog circuit with simulator

In [48], intact loop and breaking loop method are discussed to detect the presence of multiple equilibrium points. Taking breaking loop method as an example, it firstly detects the positive feedback loop; secondly breaks the loop by inserting a dependent voltage source; thirdly sweeps the voltage source linearly and checks the output voltage at its previous connected node. By checking the number of intersections between the return map which is defined as the output signal and the input sweeping signal, the number of equilibrium points can be determined. An efficient method using divide and contraction algorithm are discussed in [65]. Rather than finding all the operating points, it searches intervals that containing extra equilibrium points. If there is an extra interval where a stable operating point may exist, it detects the presence of the Trojan state. Rather than sweeping the voltage linearly as the method in [48], it runs a binary search to find the intervals. Thus, it is more efficient compared to linearly sweeping method. However, the breaking loop method only works well for circuits with only one positive feedback loop. If there are many positive feedback loops or coupled positive feedback loops existing in the circuit, multiple loops need to be broken. The computation dimension is too high to run the algorithm efficiently.

3.1.2 Temperature sweeping method

3.1.2.1 Temperature sweeping method

One way a simulator can be used to determine the presence of multiple equilibrium points is to make two dc sweeps. This takes advantage of how the simulator uses output results from one step to set the initial conditions for the next step in the sweep. This can be illustrated by considering a comparator with hysteresis. If the first sweep of the differential input starts with a large negative input and sweeps continuously in the positive direction and the second sweep starts with a large positive input and sweeps continuously in the negative

direction, the typical transfer characteristics shown in Figure 3-5(a) will be obtained. The two vertical straight lines suggest an infinite number of solutions at V_{IN1} and V_{IN2} but are not a part of the transfer characteristics but rather an artifact of the graphical representation of the simulation data. The real results from the sweep are shown in Figure 3-5(b). It shows there are at least two operating points for $V_{IN1} \leqslant V_{IN} \leqslant V_{IN2}$. Typically, the actual transfer characteristics for a simple comparator with hysteresis are shown in Figure 3-5(c). There are three operating points for $V_{IN1} \leqslant V_{IN} \leqslant V_{IN2}$.

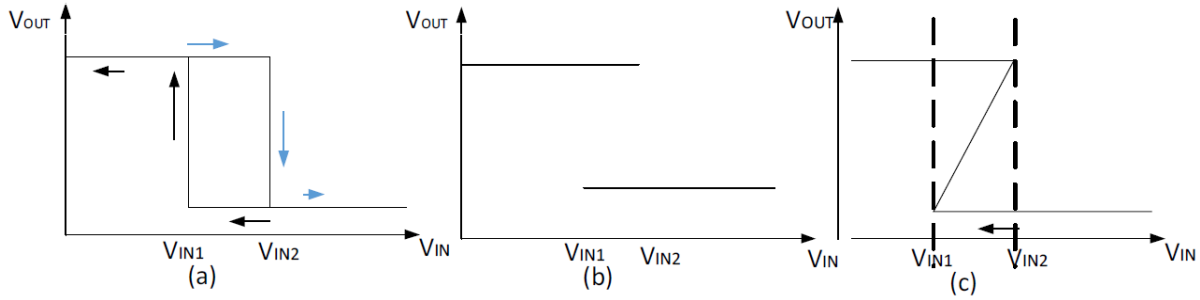


Figure 3-5 Hysteresis of the comparator

In contrast to the comparator which has a voltage input, some circuits, such as bias generators, references, and temperature sensors, do not have any electrical inputs so the option of doing a bi-directional input voltage sweep does not exist. But the temperature can be considered to be a bi-directional sweeping parameter to help the detection of extra operating points in the circuit.

The temperature sweeping method is based upon doing a homotopy-type simulation by conducting a bi-directional wide-range temperature sweep with a circuit simulator. Results similar to those depicted in Figure 3-6(a) were obtained for specific implementations of several popular bias generator and reference circuits with bi-directional temperature sweeps. These results show a hysteresis region between temperatures T1 and T2. The

corresponding typical actual relationship is shown in Figure 3-6(b) though it is a little bit tedious to obtain the region with positive slope with a simulator. This simulation shows that the circuit has 3 equilibrium points at any temperature in the interval T1<T<T2. At any temperature in the hysteresis interval, the upper and lower output voltages correspond to stable equilibrium points in the circuit and the intermediate output voltage corresponds to an unstable equilibrium point. If the temperature sweep range had been narrower, for example, from TA to TB where T1<TA<T<TB<T2, the presence of the undesired equilibrium point would typically be missed. Simulations with temperature sweeps where the simulator uses the output at the previous temperature as an initial condition for the next temperature step rather than a series of independent simulations at different temperatures are necessary to observe the hysteresis window.

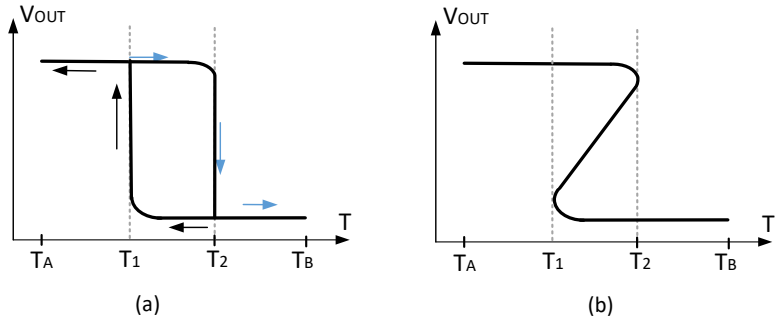


Figure 3-6 Multiple operating points characteristics in DC Temperature sweep

3.1.2.2 Effectiveness analysis of temperature sweeping method

It is shown in [66]that if a static circuit has n operating points, then (n-1)/2 operating points are unstable and between two adjacent stable operating points, there is one unstable operating point. Applying breaking loop method to all static circuits with positive feedback loops, if only positive feedback loop is broken, the return map is monotone [48]. If the circuit has more than one operating points, multiple intersections between the return map and the

input sweeping signal can be observed. To show this idea briefly, a simple circuit with only 5 transistors are taken as an example. The circuit shown in Figure 3-7 (a) is often used as a current reference [67] or a temperature sensor circuit [68]. As identified by method in the previous section, this circuit has only one positive feedback loop. It is vulnerable to multiple operating points. With one configuration, the circuit has three operating points. By using the breaking loop method, three intersections between V_{IN} and V_{OUT} corresponding to three operating points can be observed, as shown in Figure 3-7 (e). The slope of V_{OUT} at any of the intersection points are the loop gain at that operating point. In Figure 3-7 (e), operating points 'p1' and 'p2' are two stable operating points and the slope of V_{OUT} at 'p1' and 'p3' are smaller than 1; the operating point of 'p2' is an unstable operating point and the slope of V_{OUT} at 'p2' is larger than 1. For operating point 'p2', any small perturbation will make the circuit divergent from this operating point and converge to 'p1' or 'p3'. However, since the existence of multiple operating points are sensitive to PVT and components variation, with different components configuration or condition, the circuit can have only one operating point with a return map as shown in Figure 3-7(c) or Figure 3-7(g). Since the circuit's performance changes from Figure 3-7(c) to Figure 3-7(e) or from Figure 3-7(e) to Figure 3-7(g) should be continuous, with some specific configuration and condition, it exists a transition return map as shown in Figure 3-7 (d) or Figure 3-7(f) ideally, at which only one intersection point and a tangent point is present. The point of tangency is an operating point where the slope of 'V_{OUT}' is 1. Thus, there are five possible results by applying breaking loop method to the circuit in Fig.3 (a) at different conditions or configurations.

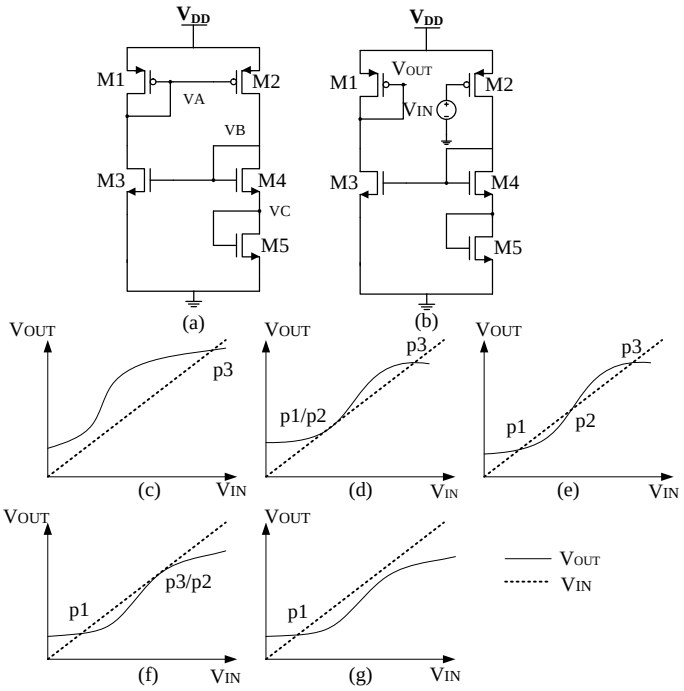


Figure 3-7 Circuit with 5 transistors and its possible return maps; (a)The example circuit;(b) breaking loop method applied on the example circuit;(c) return map with only one operating point at p3;(d) transition return map with two operating points at p1/p2 and p3;(e) return map with three operating points;(f) transition return map with two operating points at p1, p3/p2;(g) return map with one operating point at p1.

Now assuming the circuit is with a configuration or at a condition where the return map is the one shown in Figure 3-7(e) and the circuit is operating at ‘p3’. Also assuming it is possible to continuously change the configuration or condition (can be transistor’s size or temperature, etc.) while the circuit is normally operating, the circuit’s return map transfer characteristics can change from the one in Figure 3-7(e) to the one in Figure 3-7(g). Since ‘p3’ is a stable operating point, any small variation in the configuration or condition will not move the circuit from ‘p3’ to other stable operating point besides some small value change. Hence, when the configuration or condition changes continuously, the circuit will stay around the same operating point until the circuit’s return map has passed the transition one shown in Figure 3-7(f) to the one in Figure 3-7(g) where only one operating point exist.

Thus, when the circuit's configuration or condition changes slightly around the transition return map, a significant change in the operating point can be observed, from 'p3' to 'p1' in this case. For circuits with more feedback loops, more than three operating points can exist, the return maps are some different extension or superposition version of these five simple ones. When any circuit works at the operating point where the circuit's loop gain is around 1, any variation in the components configuration or other conditions making the return map go across the transition ones, a significant, discontinuous change in the operating point can be observed.

A mathematical analysis about the operating point's significant change in temperature domain is studied on this example circuit in Figure 3-7(a), showing when the circuit's loop gain equals to 1 which is when the transition return map shown in Figure 3-7(d) or Figure 3-7 (f) happens, the partial derivative of the nodal voltage to the temperature is infinity, meaning the operating point will have a significant change.

Assuming each device's current can be expressed by Equation (3-1) or Equation (3-2) depending on types of the device, then a Taylor expansion on the temperature domain of each device's current can be simplified as Equation (3-3) or (3-4) ignoring the body effect.

$$I_D = a_n f(\mathrm{V_{GS}} - \mathrm{V_T}, \mathrm{V_{DS}}) \tag{3-1}$$

$$I_D = a_p f(\mathrm{V_{SG}} - \mathrm{V_T}, \mathrm{V_{SD}}) \tag{3-2}$$

$$\mathrm{I_D} = \mathrm{I_D}(\mathrm{T_0}) + \frac{\partial I_D}{\partial V_{GS}} \frac{\partial V_{GS}}{\partial T} \Delta T + \frac{\partial I_D}{\partial V_{GS}} (-\frac{\partial V_T}{\partial T}) \Delta T + \frac{\partial I_D}{\partial V_{DS}} \frac{\partial V_{DS}}{\partial T} \Delta T \tag{3-3}$$

$$\mathrm{I_D} = \mathrm{I_D}(\mathrm{T_0}) + \frac{\partial I_D}{\partial V_{SG}} \frac{\partial V_{SG}}{\partial T} \Delta T + \frac{\partial I_D}{\partial V_{SG}} (-\frac{\partial V_T}{\partial T}) \Delta T + \frac{\partial I_D}{\partial V_{SD}} \frac{\partial V_{SD}}{\partial T} \Delta T \tag{3-4}$$

Applying these two device current equations to the circuit in Figure 3-7(a), all the equations are listed. Equations (3-5) to (3-9) are the original equations, and Equation (3-10) to (3-14) are the simplified Taylor expansions.

$$I_{D1} = a_{p1} f(\text{VDD} - \text{VA} - V_T, \text{VDD} - \text{VA}) \tag{3-5}$$

$$I_{D2} = a_{p2} f(\text{VDD} - \text{VA} - V_T, \text{VDD} - \text{VB}) \tag{3-6}$$

$$I_{D3} = a_{n3} f(\text{V}B - V_T, \text{V}A) \tag{3-7}$$

$$I_{D4} = a_{n4} f(\text{V}B - VC - V_T, \text{VB} - \text{VC}) \tag{3-8}$$

$$I_{D5} = a_{n5} f(VC - V_T, \text{VC}) \tag{3-9}$$

$$I_{D1} = I_{D1}(T_0) + \frac{\partial I_{D1}}{\partial V_{SG1}}(-\frac{\partial VA}{\partial T}\Delta T - \frac{\partial V_T}{\partial T}\Delta T) + \frac{\partial I_{D1}}{\partial V_{SD1}}(-\frac{\partial VA}{\partial T}\Delta T) \tag{3-10}$$

$$I_{D2} = I_{D1}(T_0) + \frac{\partial I_{D2}}{\partial V_{SG2}}(-\frac{\partial VA}{\partial T}\Delta T - \frac{\partial V_T}{\partial T}\Delta T) + \frac{\partial I_{D2}}{\partial V_{SD2}}(-\frac{\partial VB}{\partial T}\Delta T) \tag{3-11}$$

$$I_{D3} = I_{D3}(T_0) + \frac{\partial I_{D3}}{\partial V_{GS3}}(\frac{\partial VB}{\partial T}\Delta T - \frac{\partial V_T}{\partial T}\Delta T) + \frac{\partial I_{D3}}{\partial V_{DS3}}\frac{\partial VA}{\partial T}\Delta T \tag{3-12}$$

$$I_{D4} = I_{D4}(T_0) + \frac{\partial I_{D4}}{\partial V_{GS4}}(\frac{\partial VB}{\partial T}\Delta T - \frac{\partial VC}{\partial T}\Delta T - \frac{\partial V_T}{\partial T}\Delta T) + \frac{\partial I_{D4}}{\partial V_{DS4}}(\frac{\partial VB}{\partial T}\Delta T - \frac{\partial VC}{\partial T}\Delta T) \tag{3-13}$$

$$I_{D5} = I_{D5}(T_0) + \frac{\partial I_{D5}}{\partial V_{GS5}}(\frac{\partial VC}{\partial T}\Delta T - \frac{\partial V_T}{\partial T}\Delta T) + \frac{\partial I_{D5}}{\partial V_{DS5}}(\frac{\partial VC}{\partial T}\Delta T) \tag{3-14}$$

Since the device currents in the same branch are same, Equation (3-15) and (3-16) are obtained.

$$I_{D1} = I_{D3} \tag{3-15}$$

$$I_{D2} = I_{D4} = I_{D5} \tag{3-16}$$

For PMOS device, let's define $\frac{\partial I_D}{\partial V_{SG}} = gm, \frac{\partial I_D}{\partial V_{SD}} = gds$; (3-17)

For NMOS device, let's define $\frac{\partial I_D}{\partial V_{GS}} = gm, \frac{\partial I_D}{\partial V_{DS}} = gds$. (3-18)

Knowing Equation (3-15) and (3-16), and the definition of 'gm' and 'gds', a matrix Equation (3-19) can be obtained from Equation (3-10) to (3-14).

$$\underbrace{\begin{bmatrix} -gm1 - gds3 - gds1, -gm3, 0 \\ -gm2, -\text{gds}2 - gm4 - gds4, gm4 + gds4 \\ 0, \text{gm}4 + gds4, -\text{gm}4 - gds4 - gds5 - \text{gm}5 \end{bmatrix}}_{A} \begin{bmatrix} \frac{\partial VA}{\partial T} \\ \frac{\partial VB}{\partial T} \\ \frac{\partial VC}{\partial T} \end{bmatrix} = \begin{bmatrix} gm1\frac{\partial V_{TP}}{\partial T} + gm3\frac{\partial V_{TN}}{\partial T} \\ gm2\frac{\partial V_{TP}}{\partial T} - gm4\frac{\partial V_{TN}}{\partial T} \\ gm4\frac{\partial V_{TN}}{\partial T} - gm5\frac{\partial V_{TN}}{\partial T} \end{bmatrix} \tag{3-19}$$

The determinant of matrix 'A' in Equation (3-19) is

$$Det(A) = \text{gm}3\,\text{gm}2(\text{gm}4 + gds4 + \text{gm}5 + gds5) - (\text{gm}1 + \text{gds}3 + gds1)(\text{gds}2(\text{gm}4 + \text{gds}4 + \text{gds}5 + \text{gm}5) - (\text{gm}4 + \text{gds}4)(\text{gds}5 + \text{gm}5)) \tag{3-20}$$

Next, the loop gain of this circuit is analyzed.

Assuming the loop is broken at node 'VA', with a small input signal 'V_{Ain}' at the gate of transistor 'M2', the output signal can be obtained by the small signal analysis.

$$V_{Aout} = \frac{V_{Ain}\ gm2}{(gds2 + (gm4 + gds4) \| (gm5 + gds5))} \frac{gm3}{gds3 + gds1 + gm1} \tag{3-21}$$

The loop gain is obtained as shown in Equation (3-22).

$$Loop\_gain = \frac{\mathrm{gm3\,gm2(gm4} + gds4 + \mathrm{gm5} + gds5)}{(\mathrm{gm1} + \mathrm{gds3} + gds1)[\mathrm{gds2(gm4} + \mathrm{gds4} + \mathrm{gds5} + \mathrm{gm5}) + (\mathrm{gm4} + \mathrm{gds4})(\mathrm{gds5} + \mathrm{gm5})]} \tag{3-22}$$

When the loop gain equals to 1, the determinant of matrix 'A' can be calculated, which equals to 0.

$$\text{Thus,} \quad \begin{bmatrix} \frac{\partial VA}{\partial T} \\ \frac{\partial VB}{\partial T} \\ \frac{\partial VC}{\partial T} \end{bmatrix} = \begin{bmatrix} \infty \\ \infty \\ \infty \end{bmatrix} \tag{3-23}$$

When the circuit's loop gain equals to 1, which means the circuit is operating at p1/p2 if the return map same as the one shown in Figure 3-7 (d), or operating at p3/p2 if the return map same as the one shown in Figure 3-7(f), any change in the temperature which making the circuit's return map transfer from Figure 3-7(d) to Figure 3-7(c) or from Figure 3-7(f) to Figure 3-7(g) will make the circuit's operating point have a significant change.

Thus, if sweeping the temperature in a very large range, the circuit's return map's gradual change can go through all the transition ones; if the circuit operates around the point which is the tangent point in the coming return map, and then a significant change in the operating point can be observed abruptly. Furthermore, if sweeping the temperature forward and backward in a large range, the circuit meets two different transition return maps congaing the tangent points, and the circuit has operated at two different points which are close to two corresponding tangent points in the transition return maps respectively, a

hysteresis window can be observed in the checked output node voltage.

3.1.2.3 Applications of temperature sweeping method on circuits with multiple operating points

Several example circuits including circuits with only one feedback loop and circuits with coupled feedback loops are applied by this bi-directional temperature sweeping method, and the existence of one extra stable operating point and its vulnerable temperature range are identified by the simulation results.

To make all the simulations easy to be replicated, all the circuits in this chapter are designed and simulated in 0.5u ON and the supply voltage is 5V. The circuit in Figure 3-7(a) with configuration shown in Table 3-1 is simulated by sweeping the temperature in a very large range bi-directionally and a hysteresis window can be observed. It shows the by-directional temperature sweeping simulation result in Figure 3-8 (a). With the configuration in Table 3-1 the circuit has at least two stable operating points in temperature 53˚C to 188˚C. The real equilibrium transfer characteristic in the temperature domain with all equilibriums in the circuit is shown in Figure 3-8 (b), which can be obtained with one extra simulation and initial condition setting. The equilibrium point in the middle of the hysteresis window is the unstable operating point at that temperature. At 53˚C to 188˚C, the returned maps if obtained have the tangent point.

Table 3-1 Sizes of transistors in Figure 3-7(a)

M1	4.5u/1.8u	M2	4.5u/1.8u
M3	1.5u/4.05u	M4	8(1.5u/1.2u)
M5	8(1.5u/1.2u)		

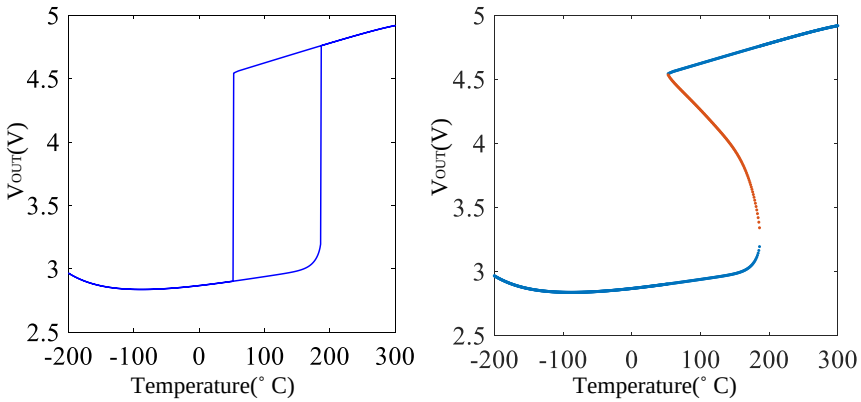


Figure 3-8 Simulation results of circuit in Fig.3(a) with size in Table 1;(a) bi-directional temperature sweeping simulation results;(b) real equilibrium transfer characteristics in temperature domain

This method can also work to detect extra equilibrium points in circuits with multiple positive feedback loops. A circuit in Figure 3-9 is simulated as examples to show the effectiveness of this method on circuits with multiple positive feedback loops.

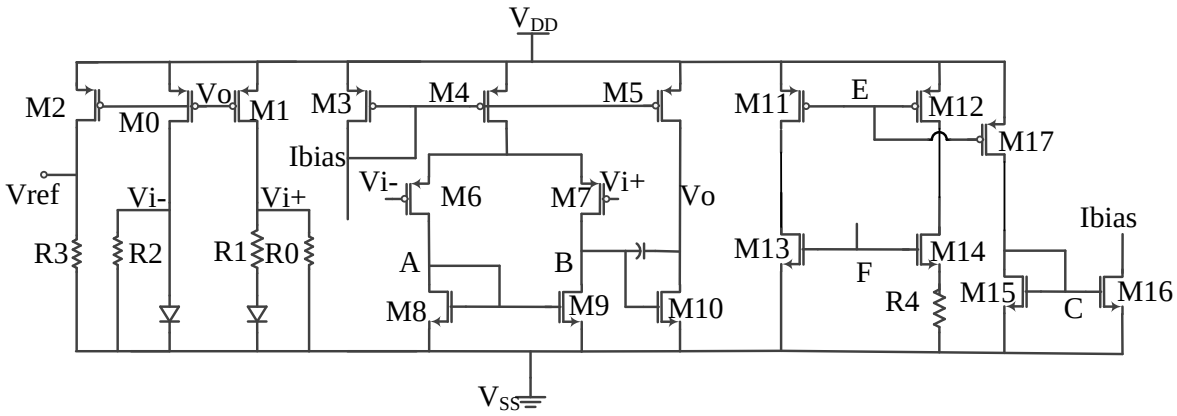


Figure 3-9 A Circuit with multiple positive feedback loop

The circuit in Figure 3-9 is simulated with size configuration shown in Table 3-2. As shown in Figure 3-10, it has at least two stable equilibrium points in temperature 63˚ to 190˚. The desired stable operating point at 'Vref' is about 1.2V and the undesired operating point is about 5V.

Table 3-2 Sizes of the transistors in Figure 3-9

M0	12u/1.2u	M1	12u/1.2u	M2	12u/1.2u
M3	12u/1.2u	M4	2(12u/1.2u)	M5	2(12u/1.2u)
M6	6(6u/0.9u)	M7	6(6u/0.9u)	M8	4(6u/0.9u)
M9	4(6u/0.9u)	M10	12(6u/1.2u)	M11	2(3u/3u)
M12	2(3u/3u)	M13	1.5u/6u	M14	2(3u/1.2u)
M15	2(1.5u/1.2u)	M16	1.5u/1.2u	M17	2(3u/3u)
R0	120K	R1	117K	R2	8.4K
R3	117K				

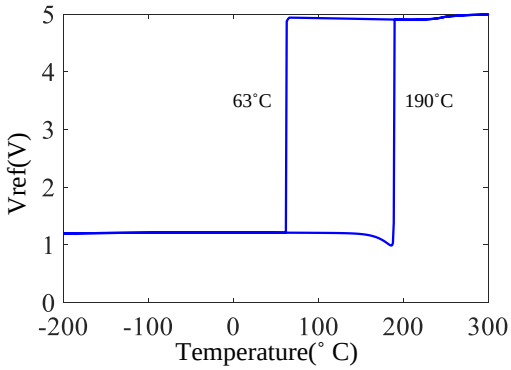


Figure 3-10 Simulation results of circuit in Figure 3-9 with size in Table 3-2

The circuit in Figure 3-11 is implemented with same size configuration of same numbered transistors in Table 3-2 and three extra transistors' sizes are shown in Table 3-3. By doing a bi-directional wide-range temperature sweeping simulation in Cadence, a hysteresis window is also observed shown in Figure 3-12 . These two circuits have multiple and coupled positive feedback loops. Using breaking loop method, at least two nodes need to be broken. Even using the method introduced in [65], the high dimensional computation makes it inefficient to detect the problem, not to say to consider the temperature's variation. But with temperature bi-directional temperature sweeping method, the extra equilibrium and the vulnerable temperature range can be easily detected.

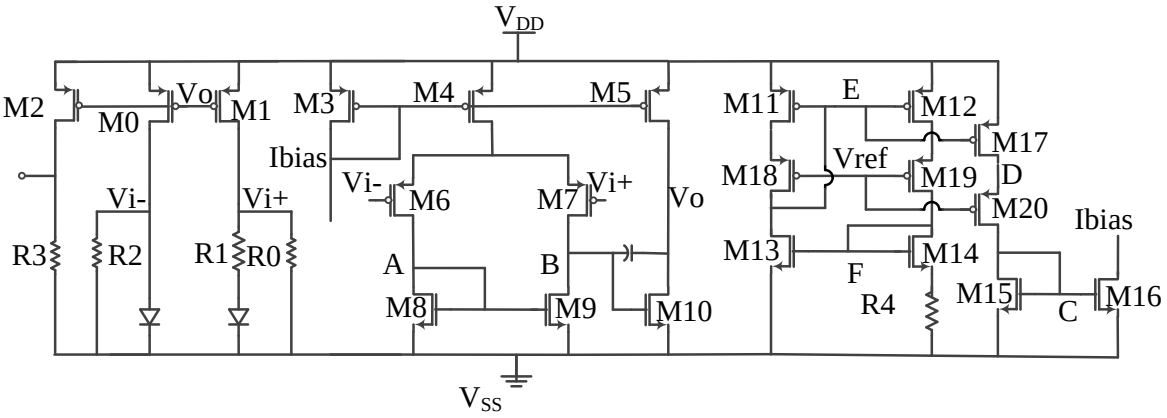


Figure 3-11 Cascode bias of circuit in Figure 3-9

Table 3-3 The three extra transistors' sizes in Figure 3-11

M18	4.05u/1.2u
M19	4.05u/1.2u
M20	4.05u/1.2u

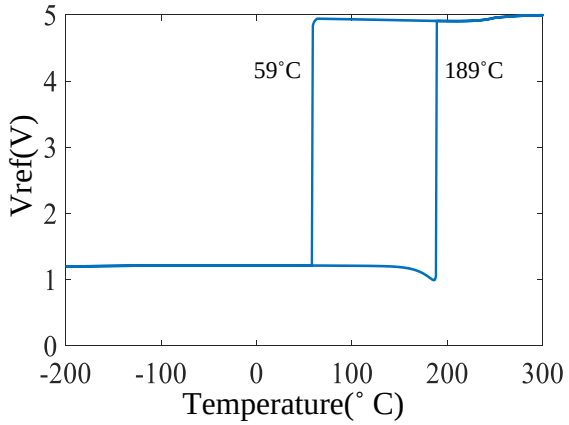


Figure 3-12 Simulation results of circuit in Figure 3-11

Examples have shown that the bi-directional temperature sweeping method can detect presence of undesired operating points in a very efficient and convenient way. It can not only show undesired operating point but also show the vulnerable temperature range where the extra operating points exist. Different to other methods trying to find all existing equilibrium points, this method only finds one extra equilibrium point. Though with more simulations

combined with some initial condition setting, other equilibrium points can also be obtained, it is already good enough by using this method since the goal is only to identify if there is at least an extra operating point existing.

3.1.2.4 Discussion on issue of temperature sweeping method

The temperature sweeping method works relying on that the circuit operates at two different operating points at the extreme low temperature and extreme high temperature. However, this method will fail to show the hysteresis window or the significantly change in node voltages if circuits have the same operating point at low temperature and high temperature, but multiple equilibrium points exist in the middle temperature range.

For the circuit in Figure 3-7(a), when sweeping the temperature forward and backward, if the circuit meets all the return maps in Figure 3-7, a hysteresis window is guaranteed to be observed. However, with some specific configuration, as shown in Table 3-4, only three of the five return maps can be met in the large temperature range, and two of them are met twice, as shown in Figure 3-13, while the real equilibrium point transfer characteristic in temperature domain is shown in Figure 3-14.

Table 3-4 Sizes of transistors in Figure 3-7(a)

M1	5(3u/3u)	M2	5(3u/3u)
M3	1.5u/3u	M4	2(1.95u/1.8u)
M5	4(3u/0.6u)		

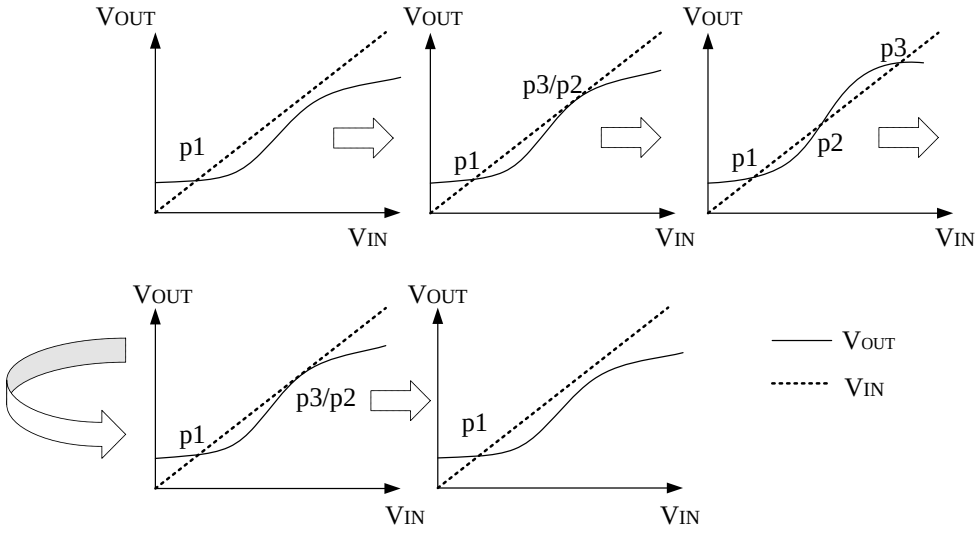


Figure 3-13 The sketch return map's transformation of the circuit in Fig.3(a) with size in Table 4 when temperature goes from low to high

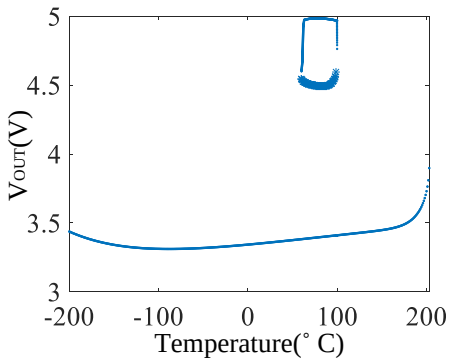


Figure 3-14 The real equilibrium transfer characteristic in temperature domain of circuit in Fig.3(a) with size in Table 3-4

By using the bi-directional temperature sweeping method on the five-transistor circuit with sizes in Table 3-4, only when the circuit is firstly operating at 'p3' or 'p2', an abruptly change in the operating point can be observed. If the simulation starts from a very low temperature firstly, the circuit should work around 'p1'. Since 'p1' is always existing and stable in all the coming return maps, the circuit will keep stay at that operating point when the temperature goes to very high and backwards to very low, and no hysteresis window or any significant change can be observed, as shown in Figure 3-14 . The undesired equilibrium

points are isolated from the desired stable equilibrium point in the temperature domain. Thus, by only using this method, the existence of multiple operating points cannot be successfully identified. But if combined with breaking loop method or other verification methods, the temperature sweeping method can still work well and speed up the verification process showing the vulnerable temperature range even if the equilibrium points transfer characteristic similar to the one shown in Figure 3-14. For example, it can be done by firstly using breaking loop method to detect the presence of extra equilibrium points at each single temperature. Once the existence is detected at one temperature, using node set to set initial condition to help the circuit converge to 'p3' and running a bi- directional temperature sweeping simulation, the verification of equilibrium's and its temperature information can be obtained.

Experiments have been done on this circuit and other circuits showing a hysteresis window can be observed by using bi-directional temperature sweeping method for circuits with most possible size configurations. The equilibrium points transfer characteristic like in Figure 3-14 has only observed in two circuit structures right now and happens only in a very narrow size configuration region.

3.2 Method to detect PAAST Trojans in dynamic system

Transient simulations with standard circuit simulators can help designers observe and analyze dynamic modes of operation of a nonlinear circuit. However, simulators provide only one operating mode with a single transient simulation. The initial conditions set at the beginning of simulation determine the mode of operation observed. Only with right setting of the initial conditions, the Trojan state can be observed. Otherwise it will always converge to the desired dynamic state in each single simulation. Thus, it is very difficult to detect the existence of Trojan modes of operation with a transient simulation. Even if it is known that a

Trojan operating mode exists, it can be difficult to verify the mode with transient simulations unless appropriate initial conditions are set. And, the problem of finding a dynamic Trojan operating mode or Trojan operating modes can be even more challenging if it is not known whether or not one or more Trojan operating modes actually exist.

3.2.1 One dynamic mode is one orbit in the phase plane

For dynamic circuits with multiple operating modes, the transient response of any circuit is completely determined by the initial conditions on all of the energy storage elements. The initial conditions are voltage on the energy storage elements. If the dynamic nonlinear system has a static Trojan state, it is one point in the initial condition domain. Any of the existing stationary dynamic modes of operation of the dynamic system is a stationary periodic orbit in the initial condition domain. If the stationary modes of operation of a dynamic nonlinear system are either equilibrium points or stationary periodic orbits, the transient response for any set of initial conditions in an arbitrarily small interval in the initial condition domain will converge to one of the stationary modes of operation. In what follows the terms “stationary periodic orbit” and “orbit” will be used interchangeably. If there are two energy storage elements, the initial condition domain is often termed as a two-dimensional phase plane. The initial condition domain can be partitioned into mutually exclusive subdomains whereby each subdomain can be associated with a unique equilibrium point or a unique stationary orbit to which the circuit will enter if a transient response starts with the initial conditions inside the subdomain. These subdomains can be viewed as domains of attraction to the associated equilibrium point or orbit. If a circuit has been designed to have a single stationary orbit, then any other stationary equilibrium points or any other stationary orbits can be viewed as a Trojan mode of operation. The phase plane for a second order nonlinear system with two stationary orbits is depicted in Figure 3-15(a).

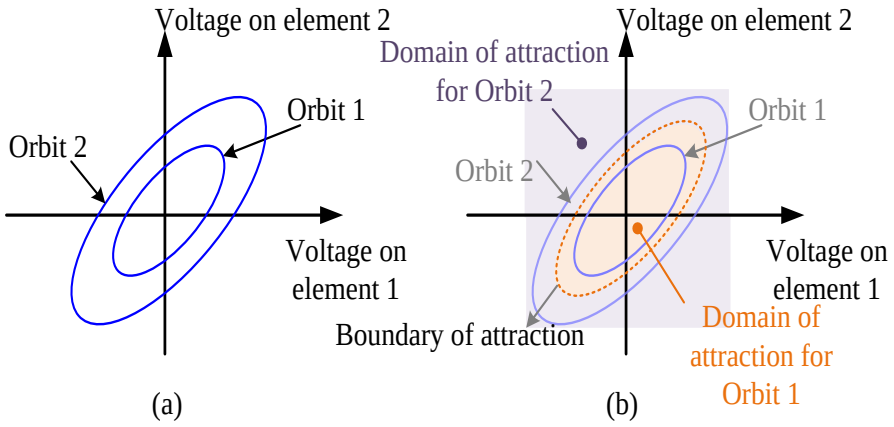


Figure 3-15 Phase plane for 2nd order nonlinear system with Trojan mode of oscillation.

If the system has two energy storage elements, both capacitors, the coordinate variables in the phase plane could be the voltage across the capacitors. If the system is designed to have a single periodic orbit, the other undesired periodic orbit corresponds to a Trojan mode of operation. In Figure 3-15(b), the domains of attraction for each of the two orbits are shown. If initial conditions on the energy storage elements are in the domain of attraction of the outer orbit, the steady state response will trace out the outer orbit and if initial conditions on the energy storage elements are in the domain of attraction of the inner orbit, the steady state response will trace out the inner orbit.

3.2.2 The sequential transient simulation with one-dimensional initial condition scanning method

If a Trojan mode of operation exists, one method of identifying this mode is to conduct a transient simulation with initial conditions that are in the domain of attraction of the Trojan mode of operation. But, since it will be assumed that it is not known whether a Trojan mode of operation exists, it is not known whether there is a domain of attraction for some Trojan operating mode. And it is also not known what region the Trojan domain of attraction is even if the existence of the Trojan is known.

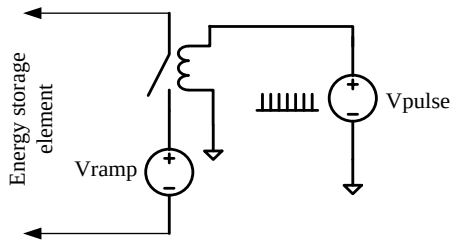


Figure 3-16 Circuit diagram to set and scan initial condition on the energy storage elements.

A simple and naive strategy that can be useful for determining whether a Trojan mode exists is to scan the initial condition domain with sufficient granularity during transient simulation such that at least one point in the initial condition scan set is in the domain of attraction of a Trojan mode. Then, by sequentially doing transient simulations using all points in this scan set as initial conditions, it can be observed from the output of the simulations whether a Trojan equilibrium point or a dynamic Trojan operating mode exists. The circuit shown in Figure 3-16 is the one used to scan the initial condition on one energy storage element during the transient simulation. The “Vpluse” generates a periodic signal with very narrow duty cycle to control the switch and set initial condition on the energy storage element. When the switch is off, the oscillator circuit is normally operating. The “Vramp” is a slow ramp signal generating the initial conditions which will be sampled when the switch is on.

Conceptually, if the system has the phase plane characteristics depicted in Figure 3-15, it would be necessary to select at least one point in the domain of attraction of the Trojan mode in the scan set. For second order dynamic circuits, orbits will often be concentric and the static equilibrium point or quiescent point will often be internal to the inner-most orbit. Thus, rather than scanning all possible initial conditions in the two-dimensional phase plane, a one-dimensional initial condition scanning with any angle to the

axis which intersects with the quiescent point of the circuit is enough to guarantee to find all the stationary modes of operation. In second order dynamic systems, the appearance of the orbit is predictable. However, for higher order dynamic systems, the shape or appearance of the stationary periodical orbits is usually unimaginable. Even, the one-dimensional linear scan would be adequate for determining the presence or absence of Trojan operating modes in second order dynamic circuits, a high dimensional transient simulation scan is usually necessary for other systems that have multiple energy storage elements, if the phase plane is more than two dimensions. In this section, the sequential transient simulation with one dimensional initial condition scanning method is presented. The one-dimensional initial condition scan can be any random angle to the axis, but in this section, the one-dimensional initial condition scan is along the axis for easy implementation and explanation. It is efficient to find all existing stationary modes in second order dynamic systems and also valid on some circuits with higher order dimensions. Two examples will be given to demonstrate this method of identifying Trojan dynamic modes. One is an analog circuit using the popular Wien-bridge oscillator architecture and the second is an injection-locked ring-oscillator that can be used for clock generation in digital systems.

3.2.3 Trojan mode identification on Wien bridge oscillator circuit

As an example for demonstrating this method of dynamic Trojan detection, consider the circuit shown in Fig.4 which is a Wien-bridge oscillator.

In an ideal Wien-bridge oscillator the gain of the base amplifier is 3 but to sustain oscillation, control signal amplitude and reduce distortion, an amplifier with a nonlinear gain is required. The gain of this base amplifier is generally greater than 3 for small outputs but less than 3 for larger outputs. A nonlinearity has been explicitly inserted into the base amplifier with the parallel diode/dc source blocks shown in the Base Amplifier of Figure

3-17. The nonlinearity is created by combinations of diodes and resistors. The dc sources are used to adjust the threshold voltage of the diodes. In this example, the nonlinearity is modeled on the resistors in the amplifier, it can also exist in the OPAMP and the resistors on the RC part. To build this example circuit with multiple stationary oscillating states existing, the nonlinearity characteristics in the base amplifier should be molded as shown in Figure 3-18. There should be multiple transfer regions existing where the gain is larger than 3 or smaller than 3.

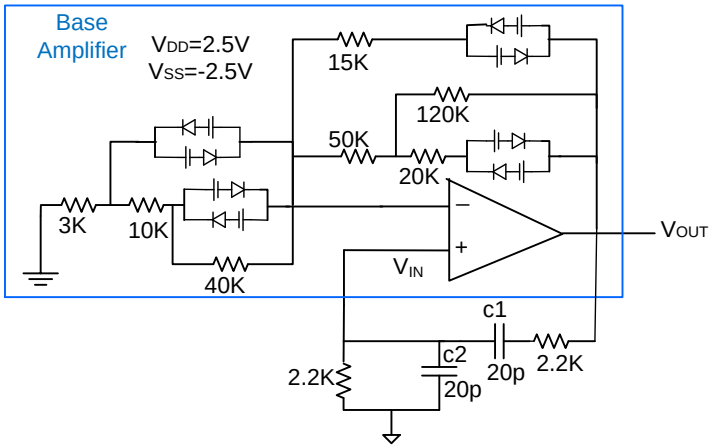


Figure 3-17 Wien-bridge oscillator circuit with three stationary dynamic modes of oscillation

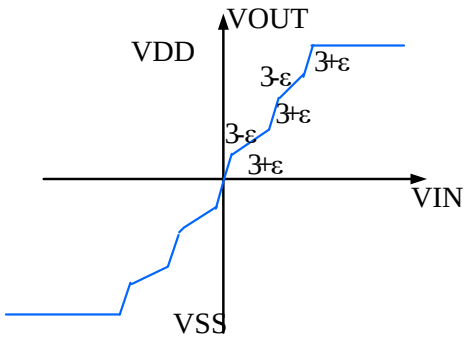


Figure 3-18 Nonlinear transfer characteristics of base amplifier

A circuit was implemented by using actual diodes in the base amplifier. The local gain (slope of transfer characteristics) of the base amplifier is shown in Figure 3-19. The

knots in the transfer characteristics that were explicitly shown in the drawing of Figure 3-18 would cause step functions in the gain with ideal diodes but the actual diodes used in the circuit resulted in the continuous gain change shown in Figure 3-19.

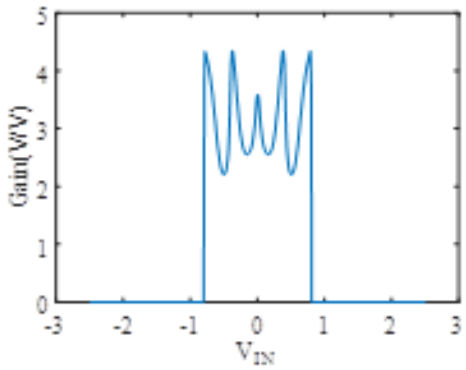


Figure 3-19 Gain of base amplifier used in prototype Wien-bridge oscillator

Since there are two capacitors in the oscillator circuit in Figure 3-17 where initial conditions can be set, a two-dimensional initial condition scan set with fine resolution could be used to identify any orbits that may exist. But since the origin is often internal to concentric orbits, a one-dimensional scan along one of the coordinate axis was used. In this circuit, the supply voltage is VSS=-2.5V, VDD=+2.5V, if the resolution of the initial condition scanning is 0.2V. It needs to run 625 transient simulations to do a two-dimensional initial condition scanning. The one-dimensional initial condition scanning will fast the detection a lot. If the common mode voltage is known as (0,0) in this circuit, only 12 or 13 simulations are enough to achieve the same results by the 625 simulations with two-dimensional initial condition scanning.

In the implementation of the sequential transient initial condition scanning method on this circuit, the one-dimensional initial condition scanning starts from VDD to VSS, containing 25 points of the phase plane, in case the common mode voltage is unknown. The

initial condition setting circuit on the two-energy storage element is shown in Figure 3-20. The 'Vpulse' generates 25 periodical 'glitches' to control the switch. When 'Vpulse' is high, the switch is on, the initial condition is sampled on C1 and C2 instantly. When 'Vpulse' is low, the Wien bridge oscillator circuit will re-start to oscillate from the new initial conditions. As shown in Figure 3-20, the initial condition sampled on C2 is always '0V' while the initial condition on C1 is swept from VSS to VDD with a resolution determined by the period of 'Vpulse'.

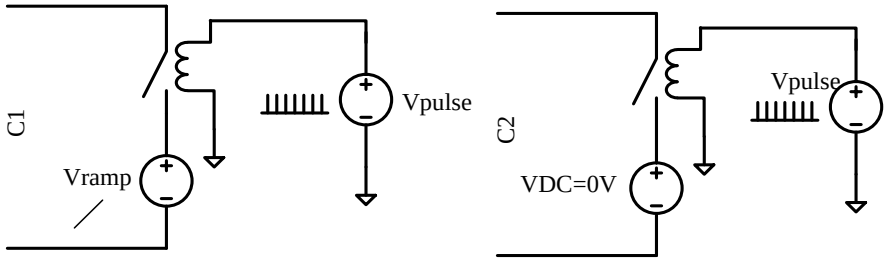


Figure 3-20 Initial condition setting circuit on C1 and C2 of Wien bridge oscillator

The initial conditions were sequentially set so that a single transient response simulation that included all 25 individual transient simulations could be run. The transient response for the entire simulation is shown in Figure 3-21. The presence of the 3 orbits is apparent by observing VOUT in this plot. An expanded segment of the transient response for each of the 3 modes at VOUT is shown in Figure 3-22. The output waveforms have only small differences in frequency but significant differences in amplitude.

The orbit results of the sequential transient one-dimensional initial condition scan is shown in a zoomed-in phase plane of Figure 3-23. To show clearly the orbits, the phase plane is only captured from -1V to 1V in x-axis, from -1.5V to 1.5V in t y-axis rather than from -2.5V to 2.5V in both x-axis and y-axis.

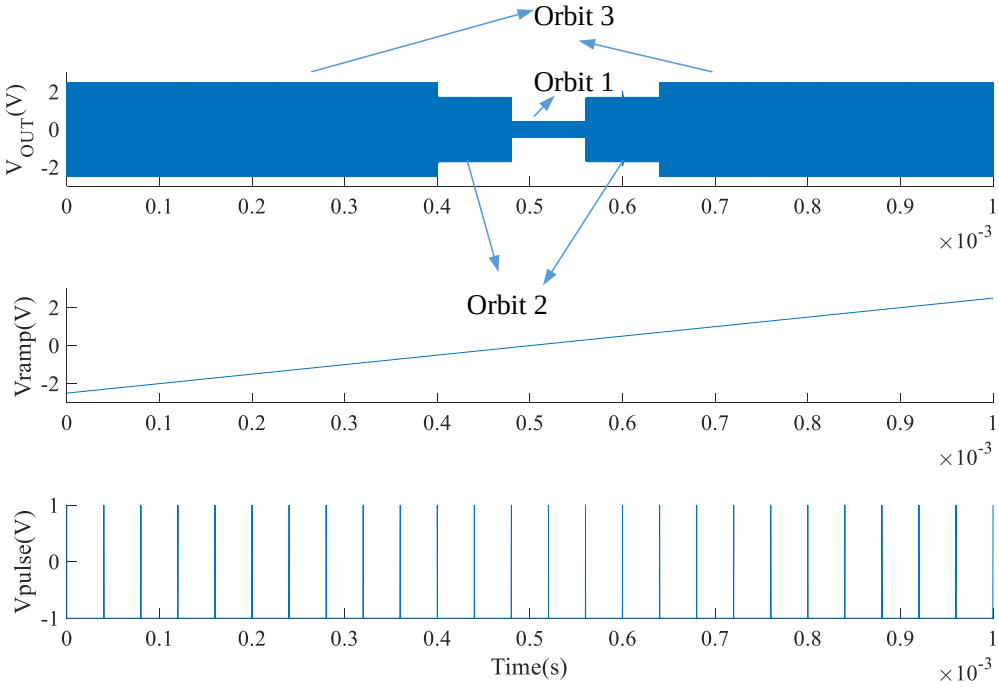


Figure 3-21Simulation results from one-dimensional scan of initial conditions

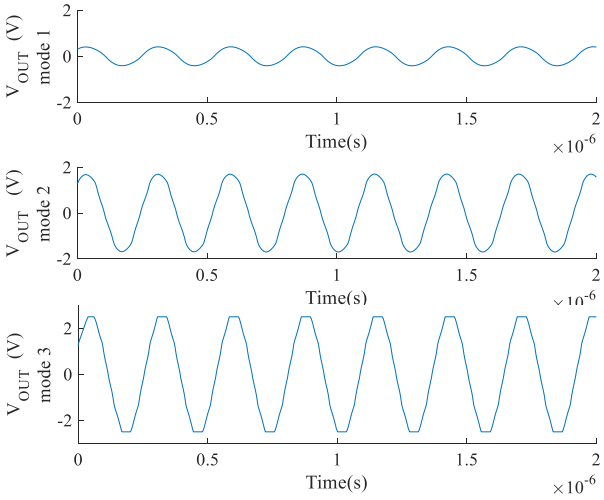


Figure 3-22 Transient response showing the three oscillating modes

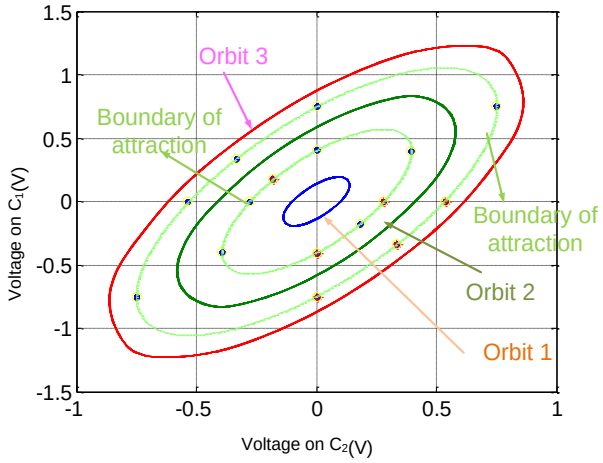


Figure 3-23 Simulated phase-plane plot for Wien bridge oscillator shown two dynamic Trojan modes of operation

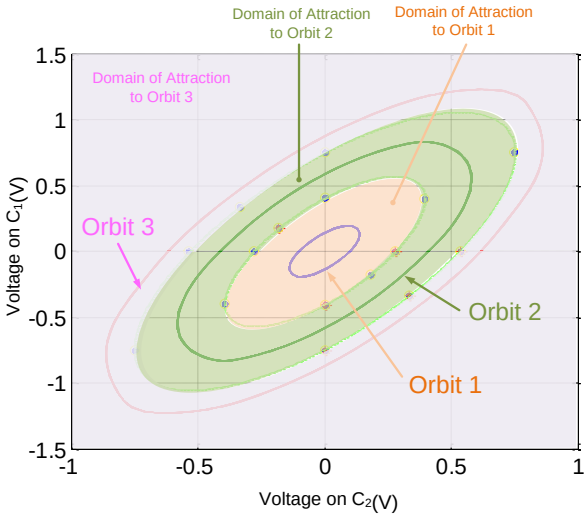


Figure 3-24 Phase plot for Wien bridge oscillator showing domains of attraction for 3 orbits

In Figure 3-23, the voltages on the capacitors C1 and C2 of the three existing dynamic modes are plotted. These simulation results show 3 orbits that differ significantly in amplitude. In this design, the desired orbit is labeled as Orbit 1. The two Trojan dynamic operating modes are denoted as Orbit 2 and Orbit 3. The corresponding domains of attraction for all three orbits were obtained by repeating the sequential transient simulation with initial conditions along different axis. They are shown in Figure 3-24. Though the domains of

attraction for the Trojan modes of operation can be quite large, designers may not naturally observe these modes during design and verification unless the initial conditions were specifically set to include a point in the corresponding domains of attraction throughout the design and verification process. . Otherwise, the circuit will always naturally converge one mode of operation and mislead the designers about the existence of Trojan modes. In the scan set, there were 25 sets of initial conditions selected corresponding to equally spaced values for the initial condition voltage on C2 with the initial condition voltage on C1 being kept at 0V. Of these 25, 2 were in the domain of convergence for Orbit 1, 2 were in the domain of convergence of Orbit 2, and the remaining 21 were in the domain of convergence of Orbit 3. Compared to the use of the naïve initial condition sweeping method which needs to run 625 transient simulations, the one dimensional initial condition transient simulation is more efficient.

3.3.4 Trojan mode identification on three stage coupled ring oscillator

Consider the injection locked ring oscillator of Figure 3-25 (c). It was reported in [46] that this circuit can have 2 modes of oscillation for some implementations of the inverters. This structure can be viewed as two 3-stage ring oscillators with one comprised of the upper three inverters in a loop and the second comprised of the lower three inverters in a loop. The two 3- stage ring oscillators are ideally identical and are comprised of inverters designated as I1 in the schematic. The injection locking is due to the symmetric cross-coupled inverters designated on the schematic with the inverters labeled as I2. It will be assumed that the drive strength of the I1 inverters is much stronger than that of the cross-coupled inverters that cause the injection locking. An implementation of the inverters that comprise the ring-oscillators designed in the AMI 0.6μ CMOS process is shown in Figure 3-25(a) with the circuit in (a) comprising the I1 inverters and in (b) comprising the I2 inverters.

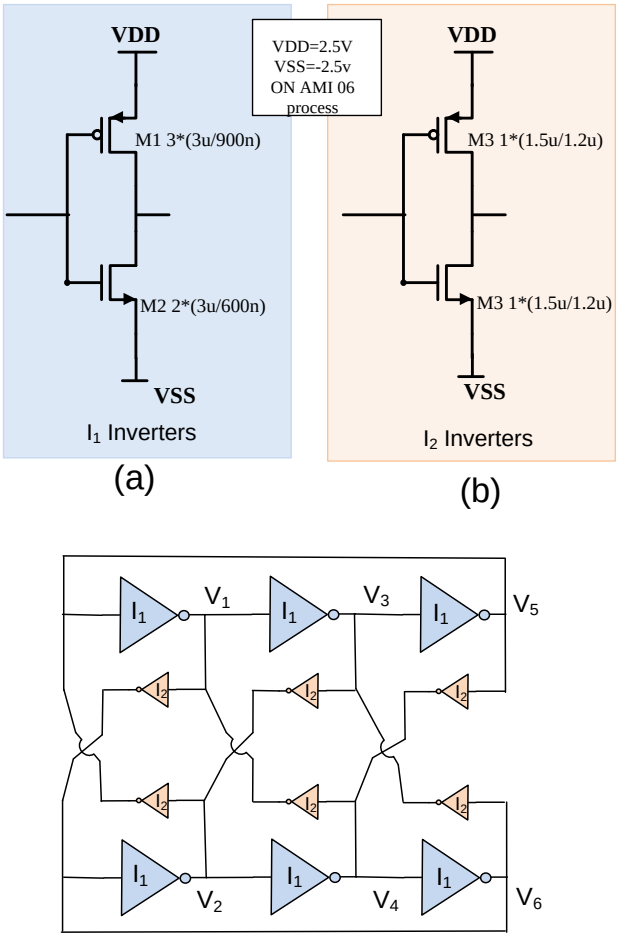


Figure 3-25 Implementation of inverters comprising injection-locked oscillator

With the basic 2-transistor inverters of Figure 3-25, the oscillator has 6 nodes labeled V1, ... V6 in addition to the biasing voltages VDD and VSS and thus the initial conditions on all capacitors can be set by setting the initial conditions on these 6 internal nodes. But since there are 6 initial condition nodes, the initial condition domain is a 6-dimensional space making it computationally impractical to scan this entire initial condition space with fine granularity. Due to the symmetric characteristics, to reduce the computational requirements, the one-dimension initial condition scan will be implemented in an attempt to identify the

Trojan modes of operation in this circuit with the goal of obtaining at least one initial condition in the domain of attraction to a Trojan orbit in the circuit.

Consider now a one-dimensional initial condition sequence $< V_1 V_2 V_3 V_4 V_5 V_6 >$ comprised of 2N initial conditions defined by Table 3-5 .

Table 3-5 A one-dimensional initial condition sequence of

	Initial Condition Sequence					
index	V1	V2	V3	V4	V5	V6
1	VSS	VSS	0	0	0	0
2	VSS+Δ	VSS+Δ	0	0	0	0
3	VSS+2Δ	VSS+2Δ	0	0	0	0
….	….	….	0	0	0	0
N-1	VDD-2Δ	VDD-2Δ	0	0	0	0
N	VDD-Δ	VDD-Δ	0	0	0	0
N+1	VDD	VDD	0	0	0	0
N+2	VSS	VDD-Δ	0	0	0	0
N+3	VSS+Δ	VDD-2Δ	0	0	0	0
….	……	……	0	0	0	0
2N-1	VDD-2Δ	VSS+2Δ	0	0	0	0
2N	VDD-Δ	VSS+Δ	0	0	0	0

where Δ=(VDD-VSS)/N is the step size and where V1 is swept first up from VSS to VDD and then down from VDD to VSS. V2 is swept first from VSS to VDD and then re-swept again from VSS to VDD. With this one-dimensional initial condition sequence, the voltage sources used to set initial conditions in the simulator can be a triangle generator V1 and a saw-tooth generator V2. One implementation of an initial condition waveform generator that can generate this input sequence is shown in Figure 3-26 where the pulse generator is used to set the sequence of initial conditions. Simulation results of a sequence of transient responses with the initial condition sequence defined above are shown in Figure 3-27. In this transient simulation, the width of the pulses that set the initial conditions were all 180ns. The ramp-up time of the saw tooth generator was 2us and the total ramp-up and ramp-down time of the triangle waveform generator was 4us. From the simulation results,

two modes can be observed by noting the small change in the amplitudes of V1 and V2 that occurs after the 2μsec mark in the transient analysis. The signal difference between V1 and V2 are generated in transient simulation which is shown in Figure 3-28, during the first 2μsec, the difference is constant as zero, which implies that the two signals are exactly overlapped. In the second 2μsec, the signal difference looks like a sinewave which means signal at V1 and V2 are out of phase. The actual time-domain waveform corresponding to the two modes for this circuit are shown in Figure 3-29. From these results the two stationary operating modes or orbits are apparent. In one mode the corresponding symmetric outputs are in-phase which is the desired mode in this design and in the other mode they are out-of-phase, which is the Trojan mode. The peak to peak amplitude of the out-of-phase orbit is about 4V and the oscillating frequency is 1.38GHz whereas the peak-to peak amplitude of the in-phase orbit is about 4.5V and the oscillating frequency is 0.97GHz.

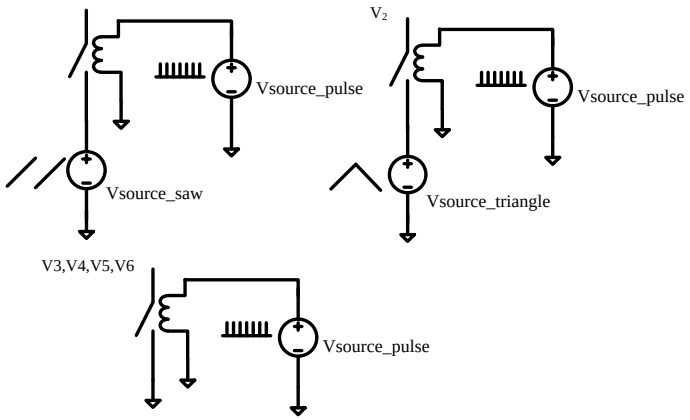


Figure 3-26. Initial condition generator circuit

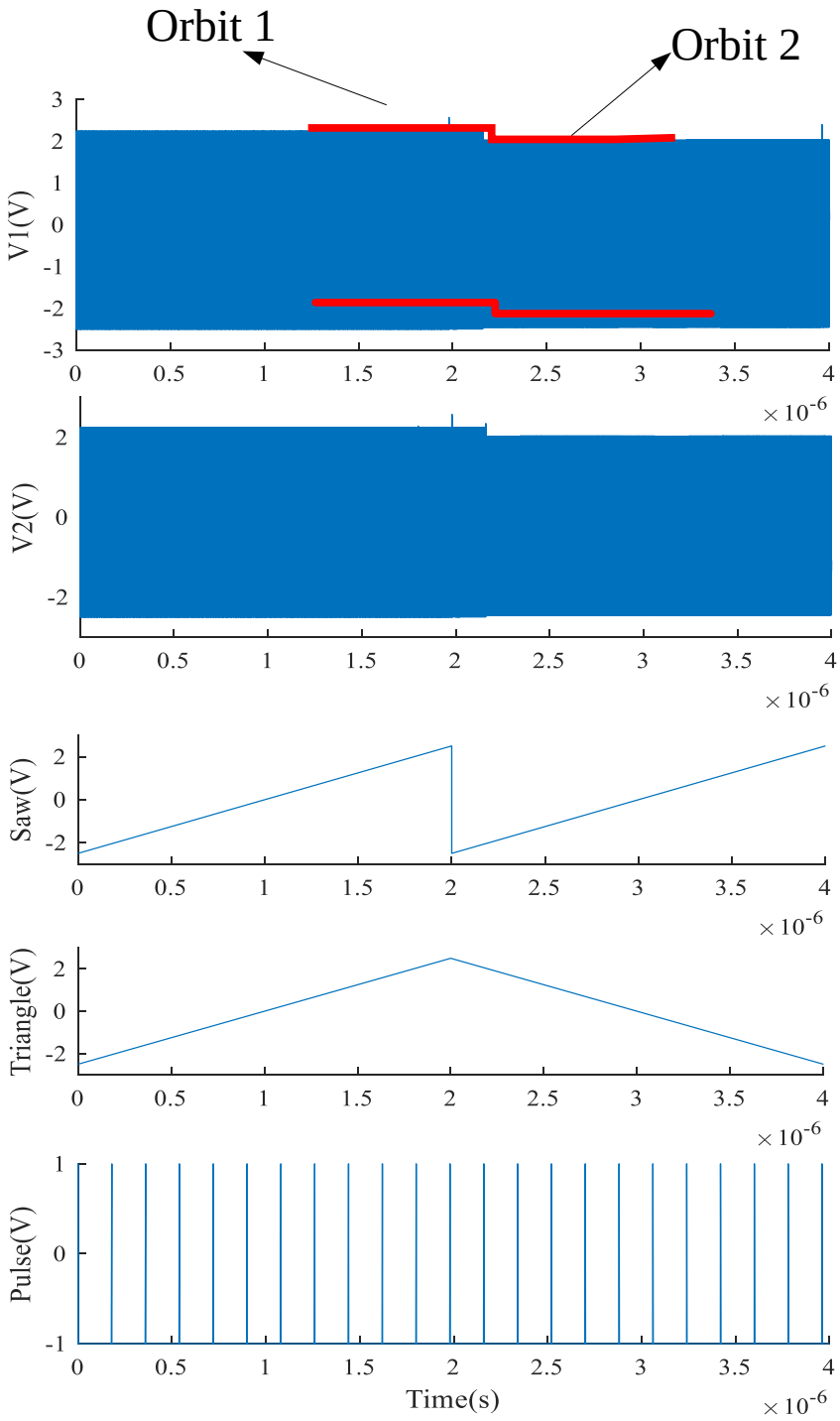


Figure 3-27 Transient simulation results with initial condition scan for injection locked 3-stage ring oscillator

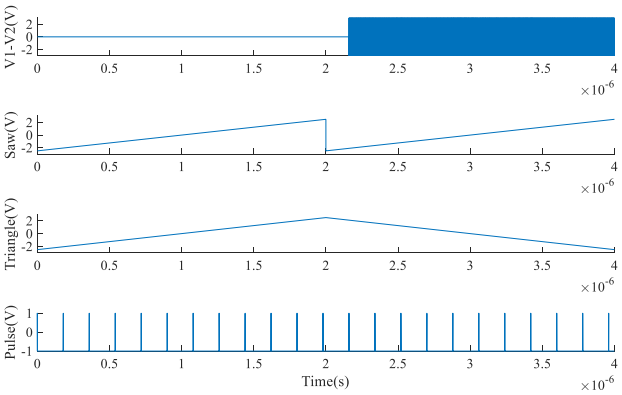


Figure 3-28 Difference between V1 and V2 in transient simulation showing 2 orbits

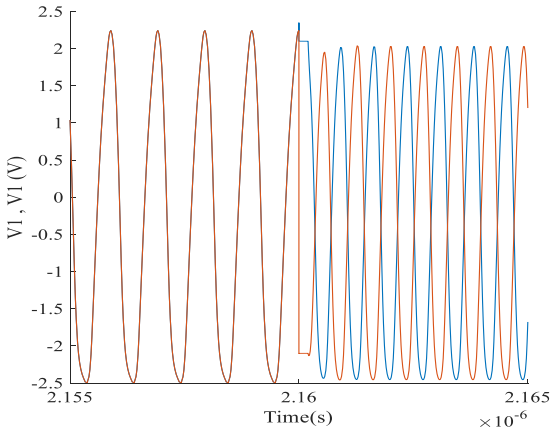


Figure 3-29 Output of oscillator at nodes V1 and V2

It was reported in [46] that this circuit has two modes (or orbits) and the initial condition-based scanning algorithm was effective at identifying these two modes. Though there is no reported evidence of any additional modes in this circuit nor any suggestion that any additional modes may exist, we cannot claim that we have found all modes in this circuit with this one-dimensional scan, but rather we can only claim that we have identified two modes with this one-dimension scanning and with this initial condition scanning resolution. If one of these two modes are the desired state, the other one is the Trojan state. By using this method, the existence of the Trojan state is being successfully identified.

The initial condition scanning method works well for nonlinear systems with two energy storage elements since the initial condition domain is at-most a 2-dimensional space. Usually depends on the circuit structure, a one-dimensional scanning is enough. It may appear that this approach will become impractical if there are a large number of energy storage elements since the size of the initial condition space will become very large. However, many useful wave-form generator circuits that may be vulnerable to the presence of one or more dynamic Trojan modes of operation will often have considerable symmetry and regularity. For example, the injection locked signal generator of Figure 3-25 (c) is symmetric from top to bottom and regular from left to right. In such structures, a practical one-dimensional initial condition scan that exploits the symmetry and regularity may often be sufficient to achieve the goal of having at least one initial condition point in the domain of attraction for each orbit. The one-dimensional scan for the injection locked ring oscillator was effective at identifying the two reported modes for this circuit.

CHAPTER 4. SIDE CHANNEL TRIGGER AND MEASUREMENT RESULTS ON PAAST TROJANS

4.1 Side channel trigger mechanism

Circuits with multiple modes of operation have been reported and concerns about the undesired modes carrying PAAST hardware Trojans were raised in previous chapters. In this chapter, trigger mechanism for PAAST Trojans will be introduced. The proposed side channel Trigger mechanism will unmask the PAAST properties. Even though the PAAST Trojans can be triggered with the addition of trigger circuits, the existence of trigger circuits could likely be used to compromise the cover of the PAAST Trojans. Although, it can also be triggered during use through noise, temperature or other operating conditions variation randomly, it is not easy to make these trigger mechanisms controllable. In this chapter, trigger methods that are also PAAST and easy to control will be introduced. These triggers are based upon a side-channel approach that can be used to trigger the Trojans on demand without any power, circuit, or area overhead. Two examples showing side channel triggers based upon PAAST Trojans incorporated as redundant dynamic operating modes of oscillator circuits will be given.

4.1.1 PAAST trigger mechanism for Wien-Bridge oscillator with embedded PAAST Trojan

It was discussed that the Wien bridge oscillator circuit of Figure 4-1 can be designed to have one or more redundant stationary dynamic modes of operation. The redundant mode or modes of operation are attributable to the specific nonlinearity in the finite-gain feedback amplifier that is used to limit signal amplitude and control spectral performance. Redundant modes of operation can also be introduced by incorporating a nonlinearity in the RC part of the circuit. For example, if the finite gain amplifier has the gain nonlinearity (magnified for

illustrative purposes) shown in Figure 4-2, the Wien bridge oscillator circuit can have two stationary dynamic modes of oscillation. The undesired oscillating mode is a Trojan mode. Since the frequency is mainly determined by the RC part of the circuit, the oscillating frequencies of these two modes are almost the same but the amplitudes of the two oscillating modes can be very different. Simulation results showing the two modes of operation obtained from an implementation of this circuit are shown in Figure 4-3. The nonlinearities in the finite gain amplifier were introduced by incorporating diode limiters (not shown) in the resistor R1'. In this design, the desired mode has a peak to peak amplitude of 2V while the peak to peak amplitude of the Trojan mode of oscillation is approximately 5V.

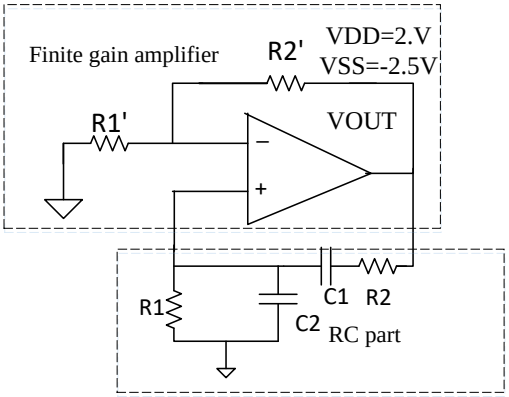


Figure 4-1 Wien bridge oscillator

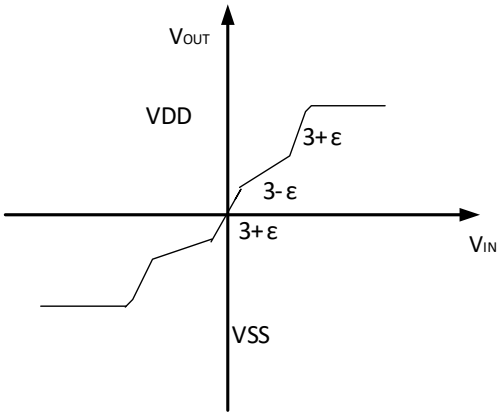


Figure 4-2 Soft nonlinearities in the amplifier

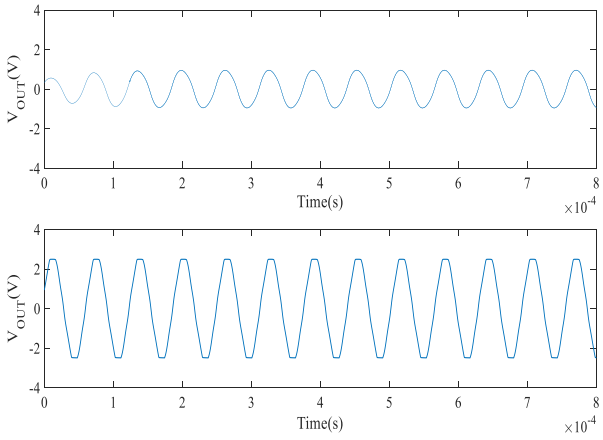


Figure 4-3 Two operating modes of Wien bridge oscillator

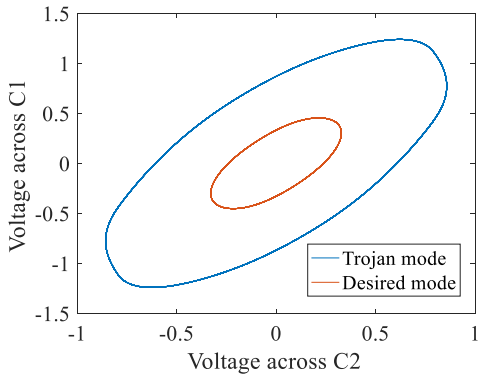


Figure 4-4 Orbits of Wien bridge oscillator

When the supply voltage of this circuit normally ramps up, the circuit will naturally converge to the desired operating mode due to the fact that when the circuit is off, the initial conditions on the two capacitors are naturally set to around 0V which is inside the inner orbit and thus inherently in the domain of attraction of the desired mode of operation as can be seen from Figure 4-4. Even with considerable noise present during start-up, the circuit will still converge to the desired state since the initial conditions are far away from the domain of attraction of the Trojan mode of operation. Thus, during standard simulations and verification

as well as standard testing, the circuit will invariably show operation in the desired mode making it difficult to even be aware of the existence of the Trojan mode of operation. However, the Trojan state really exists and can be triggered on demand with a side-channel trigger during its normal mode of operation.

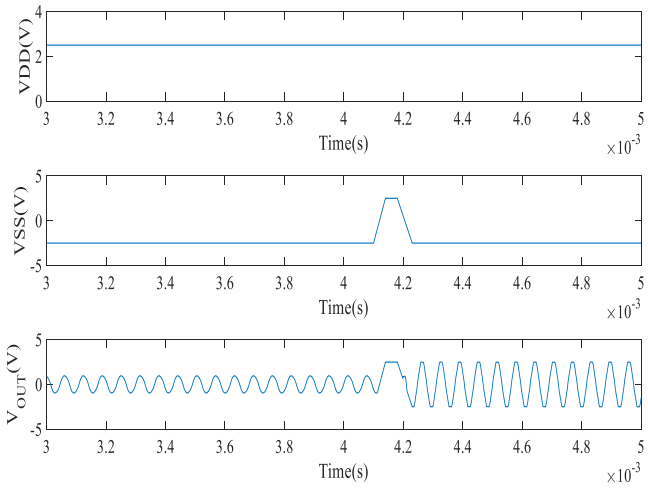


Figure 4-5 Side-channel trigger of Wien bridge oscillator

Figure 4-5 shows simulation results of a specific side-channel trigger. The trigger is based upon applying a pulse of specific height and width on the VSS bus. Prior to triggering, the circuit is operating in the desired oscillation mode with a peak to peak amplitude of 2V. After triggering the circuit is operating in the Trojan mode with a peak to peak amplitude of 5V. This pulse on the VSS bus establishes an initial condition on the energy storage elements that is in the domain of attraction of the Trojan operating mode and this is what causes the circuit to transition from the desired mode to the Trojan mode when the side-channel trigger is applied.

Though not shown in the simulation, a side channel trigger can also be used to trigger the oscillator to switch between the Trojan mode and the desired mode of oscillation. Thus, an adversary could momentarily switch the circuit to operate in the Trojan mode and then

return it to operate in the desired mode. If this were to occur, it might be difficult for the user to even recognize that the circuit operation had been compromised yet the payload may have been delivered during the time interval when it was operating in the Trojan mode.

It should be apparent that this side-channel trigger mechanism is power, area, architecture and signature transparent. Since both the Trojan and the trigger mechanism are PAAST, detection of the Trojan can be extremely challenging. Though this example has a domain of attraction to the Trojan state that is rather large, judicious design of the circuit can make the domain of attraction of the Trojan mode arbitrary small making detection even more difficult.

4.1.2 PAAST trigger mechanism for three-stage injection-locked oscillator with PAAST Trojan

As reported in Chapter 3, the circuit in Figure 4-6 can be designed to have two oscillating modes. In one mode, the signals at nodes 'V1' and 'V2' are in-phase while in the other mode the signals at nodes 'V1' and 'V2' are 180˚ out of phase. Besides the difference in phase, the oscillating frequency and peak to peak amplitudes are also different. When the circuit is in use, if the desired mode is the first mode described above, then the Trojan mode is the one where the signals at 'V1' and 'V2' are out of phase. Likewise, if the desired mode is the second mode, then the Trojan mode corresponds to in-phase signals. In this work, it will be assumed that the circuit has been designed to generate two oscillating signals which are 180˚ out of phase. An implementation of the circuit designed in a 0.5µm CMOS process is shown in Figure 4-6. In this implementation, the circuit will naturally start up to the desired state which signals are out of phase at node 'V1' and 'V2'.

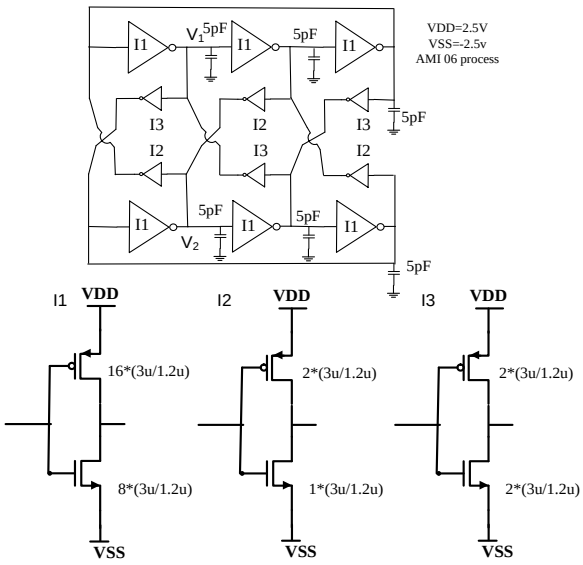


Figure 4-6 Implementation of injection-locked ring oscillator

Additional capacitors have been added to all nodes in the circuit to make the oscillating frequency easy to control. Thus, when the supply voltage naturally ramps up, the circuit will naturally converge to the desired oscillating mode. Even with noise existence, the circuit is robust to start up to the desired mode of operation. By using standard simulator to verify the circuit, only the desired oscillating mode can be observed; the existence of the Trojan mode is unknown to the designers. When the circuit is normally started up and operated in the desired mode, by using a PAAST side- channel trigger mechanism on the supply bus, the circuit can be triggered to the Trojan mode on demand.

Simulation results of this oscillator are shown in Figure 4-7. After start-up, the circuit is operating in the desired mode where the signals at nodes ‘V1’ and ‘V2’ are out of phase with peak to peak amplitude and oscillating frequency of 4V and 55MHz respectively. By applying a pulse to the VSS supply bus at ‘t=1.4usec’ of duration 30nsec, the oscillator is triggered into the stationary Trojan mode of operation where the signals denoted as ‘V1’ and ‘V2’ are in phase and with peak to peak amplitude and frequency of 4.8V and 38MHz

respectively. This serves as a side-channel trigger for this injection-locked oscillator. During the period when the trigger is added to the supply bus, all the inverters are out of function and voltages across the parasitic capacitors are being reset. After the supply voltage comes back to the normal level, the circuit's final oscillating state is determined by the new initial conditions, Thus, it can change from the desired state to the Trojan state. Though not shown in the simulation results, a second side-channel trigger pulse can be used to trigger the circuit to return to the desired mode of operation.

In this injection locked three stage ring oscillator circuit, the existence of Trojan modes is inherently because of its coupled and injection locked structure. In some applications, injection locking technique is used to eliminate clock skews around a large chip area or to generate quadrature phase signals. In coupling the oscillator circuits, the desired performance can be achieved but a Trojan oscillating mode is introduced without knowing. Since there are no extra circuits added to insert Trojans or for trigging mechanism, these types of Trojans with the side channel trigger mechanism are transparent to power, area, circuit architecture and signatures.

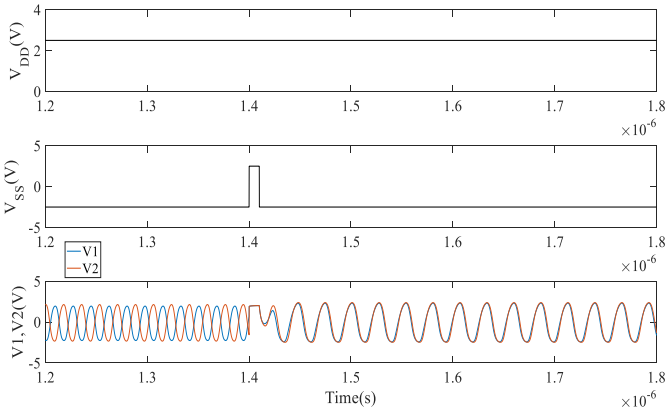


Figure 4-7 Side-channel trigger of injection-locked ring oscillator

4.2 Measurement results of PAAST Trojans in two dynamic circuits

Two dynamic circuits introduced in this dissertation are built with commercial products and measured in lab. In each of the circuits, two oscillating states can be observed, and once Trojan trigger mechanism is applied during the normal operation, the circuit's oscillating state will change from the desired one to the Trojan oscillating state.

The Sallen-key structure-based oscillator circuit is built with UA741 OPAMP, resistors, capacitors and diodes. The nonlinearity in the amplifier shown in Figure 4-8 is generated by the combination of resistors and diodes. The measured result shown in Figure 4-9 displays when the trigger mechanism is applied, the oscillating state changes from the normal state to the Trojan state. The two oscillating states have significantly different amplitudes. In this circuit, the large amplitude state is assumed as the desired state, and the state with small peak to peak amplitude is the Trojans state. In Figure 4-9, it shows a one-second-long measurement results in Figure 4-9 (b) and two zoomed in results in Figure 4-9 (b) and (c). In Figure 4-9 (b) and Figure 4-9 (c), it shows that during normal operation the circuit can be triggered to Trojan state, and it can also be triggered back to the desired state.

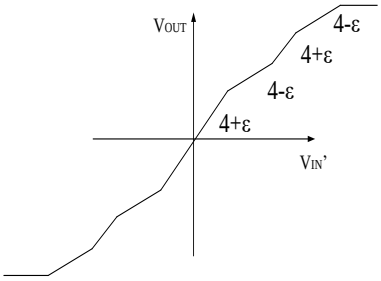


Figure 4-8 Amplifier's gain nonlinearity in the measured Sallen key based oscillator

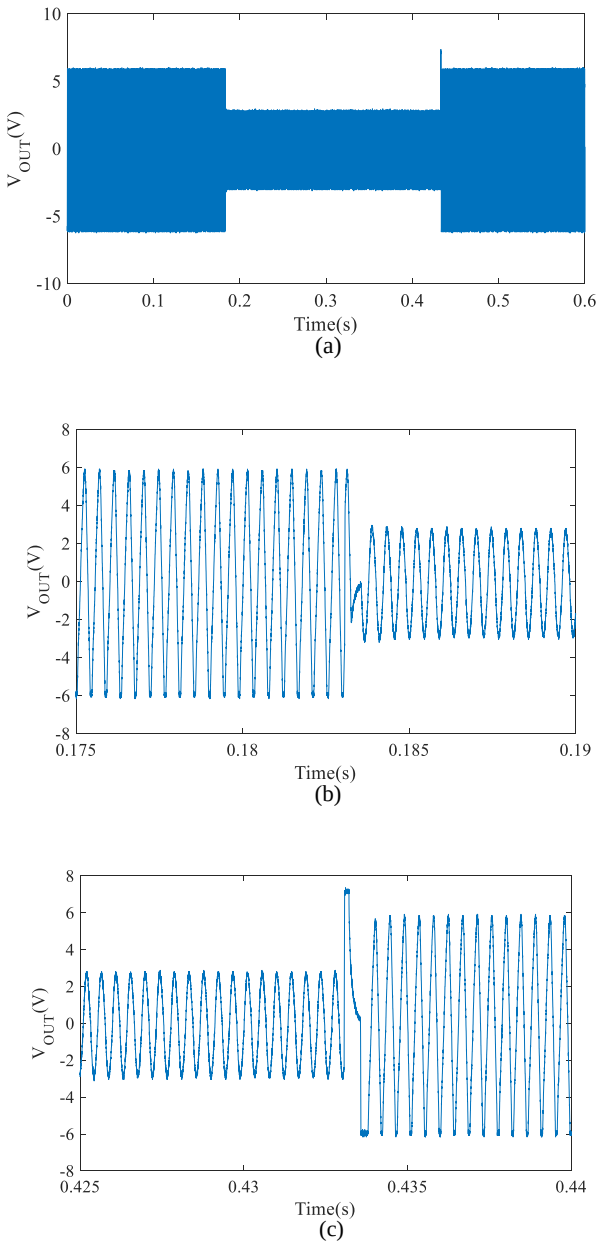


Figure 4-9 Measurement results of Sallen-key structure based oscillator circuit; (a) Measurement results for the whole triggering time;(b) results of triggering the circuit from normal mode to Trojan mode; (c) results of triggering the circuit back to normal mode

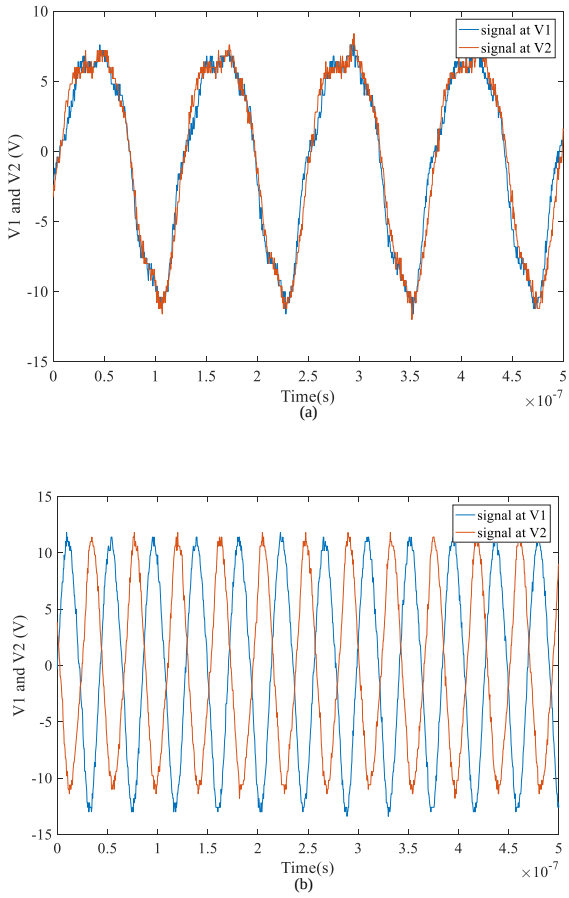


Figure 4-10 Measurement results of three stage coupled ring oscillator circuit; (a) in-phase mode; (b) out of phase mode

A three-stage coupled ring oscillator circuit is implemented with multiple CD4049UB devices, which are inverting hex buffers. As shown in Figure 4-10, two oscillating states are observed. For the measured results in Figure 4-10 (a), it shows the oscillating signals at 'V1' and 'V2' are in phase, and the oscillating frequency is about 8MHz. However, when the initial condition changes, a second mode of operation can be triggered as shown in Figure 4-10. Signals at 'V1' and 'V2' are 180˚ out of phase, and the oscillating frequency is around 23MHz.

Shown by the two built circuits and the measured results, Trojans in analog circuits can be easily inserted, and without any extra circuitry, area, power overhead. Once triggered,

the circuit will work at the Trojan state and result in severe problems. Additionally, the adversary can trigger the Trojan to occur only in a very short of time and then trigger it back to the normal state as shown in Figure 4-9 (c), making it more difficult to detect even it has already been triggered.

CHAPTER 5. COUNTERFEIT COUNTERMEASURES WITH SUBTHRESHOLD AUTHENTICATION UNDER-CIRCUITS

To reduce the entry barrier for COTS manufacturers to include authentication circuitry and eliminate the financial incentives for the production of counterfeit countermeasures, a PUF (Physical Unclonable Function) circuit which can generate random bits of sequence for authentication is proposed. The PUF circuit is a circuit which is unclonable because of the physical mismatches on each PUF cell is random. By exploiting the physical mismatches, unique code sequence as a fingerprint for the IC can be generated.

What is unique in the proposed approach is not the PUF but the proposed solution requires no additional pins, no silicon area overhead, and does not affect the normal operation of the circuit. Furthermore, once a basic authentication core is created, the approach should be directly applicable to a wide range of COTS components over multiple technology nodes with little or no additional design effort required. This will be realized by utilizing the area underneath existing bonding pads to build an "under-circuit" and using existing pins for reading the fingerprint obtained from the PUF. To avoid affecting the characteristics of the original device, the PUF circuit will turn itself off when a circuit receives a normal supply voltage. The PUF circuit along with its I/O will be activated when the supply voltage is around one half the normal 'Vdd' by operating all devices in the under-circuit in the subthreshold (weak inversion) region.

Traditional PUF circuits often take advantage of a group of multi-paralleled delay paths to generate the unique key sequence [69][70]. In this implementation, the core of the PUF circuit is a dynamic shift register loop operating in weak inversion region with a latch cell [71] as the PUF unit. Depending on the physical random mismatches on DFF's, it can generate a unique key directly without any use of the delay timing comparison or any MUXs.

Besides the supply, it doesn't need extra 'Challenge' to weak up the PUF circuit. Thus, no input pin is needed. The PUF circuit will be powered when the supply voltage is around one half of the normal supply, where the COTS IC usually doesn't work. It uses the original IC's supply, ground, and output pins without any disturbance to the IC's normal performance. Hence, this PUF circuit doesn't need any extra pins and it has almost no interaction with the COTS IC circuit during normal operation. The authentication under-circuit was designed in an IBM 0.13u process with a normal supply voltage of 1.2V. The total area for the authentication under-circuit comprised of a 20-bit comma and a 64-bit PUF is around 90umx90um, which is about 85% of the area required for a single bonding PAD in this process.

5.1 The operation of the authentication under-circuit

A block diagram of the authentication under-circuit is shown in Figure 5-1. The 3-pin authentication circuit shares the supply pin, a digital output pin, and ground pin with those of the original IC. A threshold trigger circuit is set to trigger around 75% of the normal supply voltage and is used to turn on three PMOS switches to activate the under-circuit. The clock circuit is a weak inversion ring oscillator and is used to clock the shift register loop to the output. The shift register loop is designed with a sequence of flip flops. The initial condition on all flip flops in the shift register are determined by random mismatch of minimum-sized inverters, thus the shift register is actually also the PUF circuit. A fixed sequence generated by deterministic DFF's appended in the shift register loop will serve as a "Comma" for extra sequence head detection.

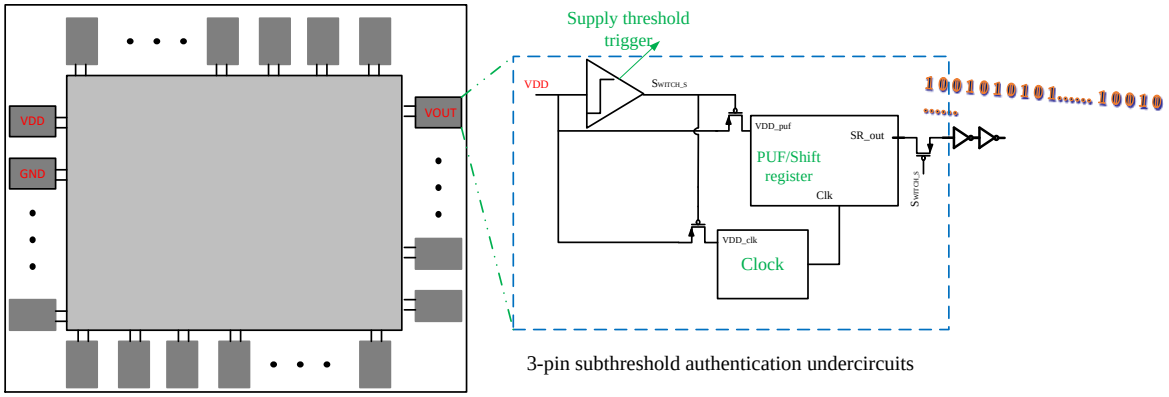


Figure 5-1 The implementation diagram of authentication circuit

If the applied voltage is at the normal IC supply voltage, the threshold trigger circuit outputs a high-level signal that controls the PMOS switches. These switches will prevent the shift register based PUF circuit and the clock circuit from drawing power during the IC's normal operation and also prevent the PUF circuit from affecting the output of the IC. This isolation allows the authentication circuit to share the same pins as the IC, which saves on die area and packaging costs. Once the supply voltage is set around half of the normal supply, the switches are activated, providing power to the shift register loop circuit and the clock circuit. The shift register loop based PUF circuit will generate the unique sequence for authentication depending on the initial conditions of the DFF's. The DFF's in the shift register loop can be divided into two segments. The initial conditions on one segment's DFF's are determined by random mismatches, while the initial conditions of DFF's in the other 'Comma' segment are previously determined by size configurations.

The designed PUF circuit will generate 64 random bits for each IC. However, the efficient number of bits for authentication doesn't need to be exact 64. For authentication, a very strong PUF which generates same 64 bits of code in different tests is not necessary. Because of the noise or temperature variations, there could be several bits from a PUF circuit

varied in different test. If a code sequence from a customer and a code in the database are close enough, or critically saying the hamming distance between them is smaller than a tolerated hamming distance, the device from the customer will be authenticated. The hamming distance is defined as the number of bits different from two code sequences, $H_N = \sum (b_{i1} - b_{i2})^2$.

In this chapter, the detailed implementation and statistical analysis of the authentication under circuit will be discussed.

5.1.1 Supply threshold trigger circuit

The threshold trigger circuit is a circuit which produces a control signal to turn on the PMOS switches when the supply is around half of the normal 'Vdd' and turn off the switch when the supply is at the normal level. The threshold trigger circuit is designed by exploiting the threshold property of the inverter. The schematic in Fig.2 shows the implementation of this threshold trigger circuit.

As shown in Figure 5-2, the first stage of the threshold trigger circuit is a voltage divider including two NMOS transistors which are sized such that the output of the stage is lower than half of the supply voltage (VDD) when VDD is low, but is higher than half of the supply voltage when VDD is higher than some value.

The second stage and third stage consists of two inverters to create the required trigger signals. The inverter constructed by M3 and M4 has a threshold voltage around half of 'VDD'. As shown in Figure 5-3, when the supply voltage is low, the signal 'V0' is lower than the threshold voltage of the inverter constructed by M3 and M4. Therefore, the signal 'V1' will follow the supply voltage. As the supply voltage continues to increase, the signal 'V0' becomes larger than the threshold voltage of the inverter constructed by M3 and M4,

thus V1 decreases. When the supply voltage is large enough, and V1 is smaller than the threshold voltage of the third inverter, the third inverter will change its state from low to high. For the supply threshold trigger circuit implemented in this paper, the threshold voltage is around 900mV. When the supply voltage is normal value with 1.2V in this process, the output of this threshold circuit is high. When the supply voltage is 0.6V, the output voltage is low, and the PMOS switches in Figure 5-1 will be turned on. With the help of this circuit, the original COTS IC and the authentication circuit can be isolated when the supply is normal, and the PUF circuit can generate the unique authentication code when the applied voltage is half of the normal supply.

The transistors of M1, M2 are sized with large multipliers to minimize the variations due to mismatches. Additionally, the threshold voltage of this trigger circuit is designed for around 75% of the normal supply; it has enough distance away from both 1.2V and 0.6V. Monte Carlo simulations have been done at room temperature to show for 200 simulations, the trigger voltage varies from 0.83v to 1.02V and it is still larger than the half supply and lower than the normal supply, as shown in Figure 5-4(a). Simulations with temperature variations have also been done. In Figure 5-4(b), it shows the trigger voltage varies from 0.82V to 1V at temperature region from 0˚C to 80˚C. With different mismatches or at different temperatures, the voltage trigger circuit can guarantee to turn off the PUF circuit while the supply is around 1.2V and turn on the PUF circuit while the supply is around 0.6V. Therefore, it is robust to mismatches or temperature variations.

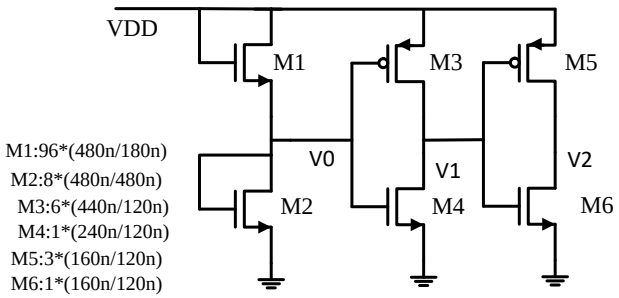


Figure 5-2 Block Diagram of Threshold trigger Circuit

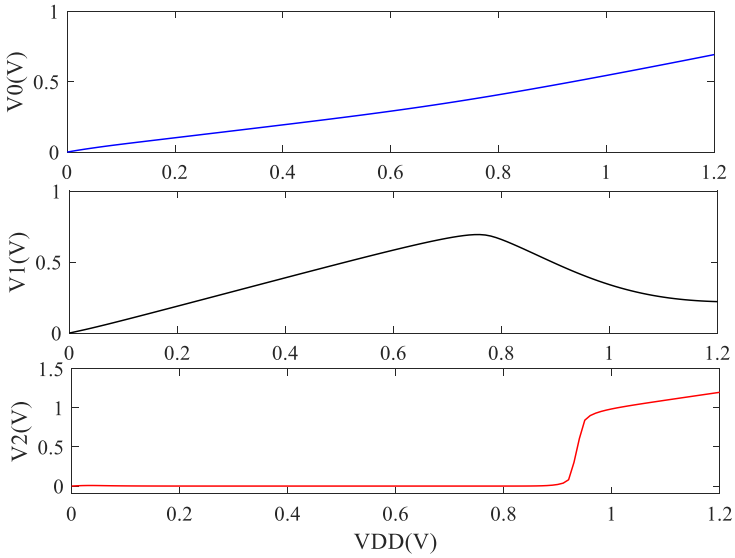
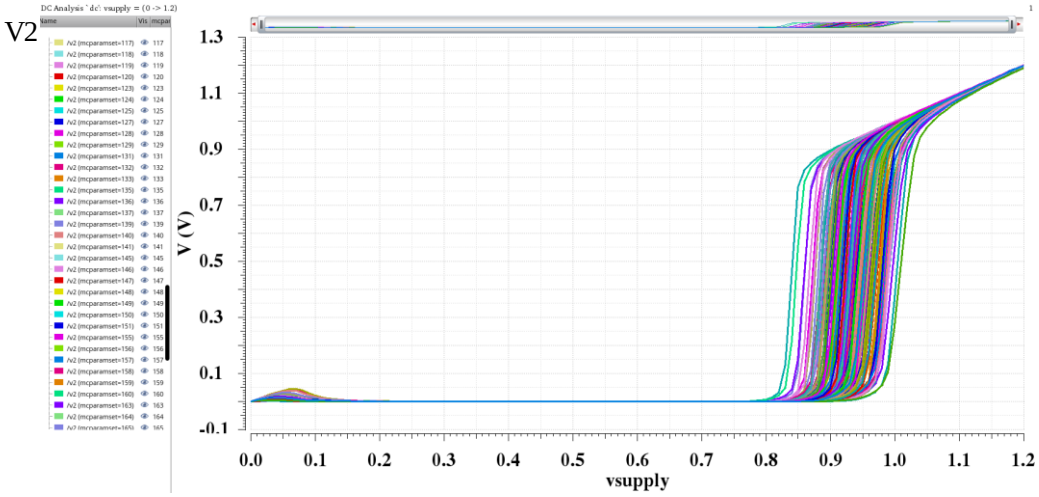
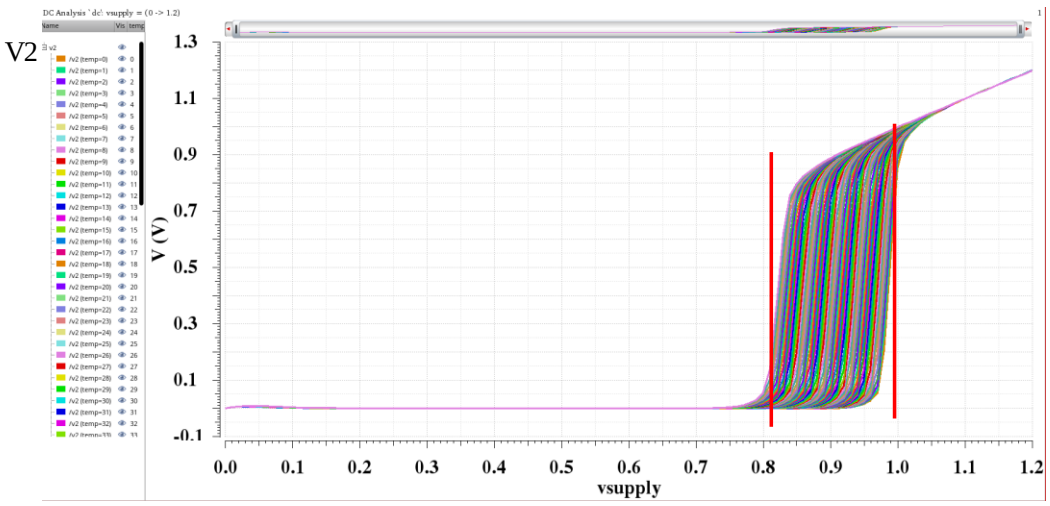


Figure 5-3 The transfer curve of the supply threshold trigger circuit



(a)



(b)

Figure 5-4 (a)Monte Carlo simulation results of the threshold trigger circuit;(b) simulation results of the threshold trigger circuit at different temperatures

5.1.2 PUF cell

Several silicon-based PUF cell implementations have been well studied. One commonly used one is a delay-based arbiter PUF cell. The idea is to exploit the variationes in two 'identical' path delays to generate a signature bit. There are also other PUF cells based on variations on ring oscillator's oscillating frequency or transistors' threshold voltage. The PUF cell used here is a latch circuit with back-to-back connecter inverter structure. As shown in Figure 5-5, it usually constructed by two identical inverters. During the supply ramping up, the offset on the inverter due to random mismatches will determine the initial state at node 'Q'. When the circuit is powered up, the signal at node Q can be high or low depending on the offset of the two inverters. During the design phase, the two inverters in the D-latch are designed with the same sizes. Due to process variations and mismatches, the two inverters would not be exactly symmetric. The offset on the two inverters will determine the initial condition of the latch. For each DFF, the mismatches on the inverters are random and

unrelated to other DFF's. Thus, the initial condition of any latch is either high or low and is totally independent of other devices. Each latch has an equal probability which is 0.5 that its initial condition at node Q is either high or low.

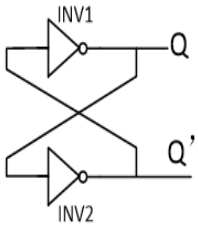


Figure 5-5 Latch based PUF cell

The latch based PUF cell consumes less area and devices; most importantly it is inherently contained in many DFF circuit. Build the PUF circuit with DFFs based shift register circuit, not only the random unique signature bits can be generated with the latch cell, but also extra shift register circuit are not needed for the output of the PUF sequence.

The DFFs used in the Shift register are transmission gate-based master-slave D flip flop circuit which is shown in Figure 5-6. Two-phase non-overlapping clock needs to be used to control its operation. Depending on the clock signals, either the master latch or the slave latch will be turned on separately.

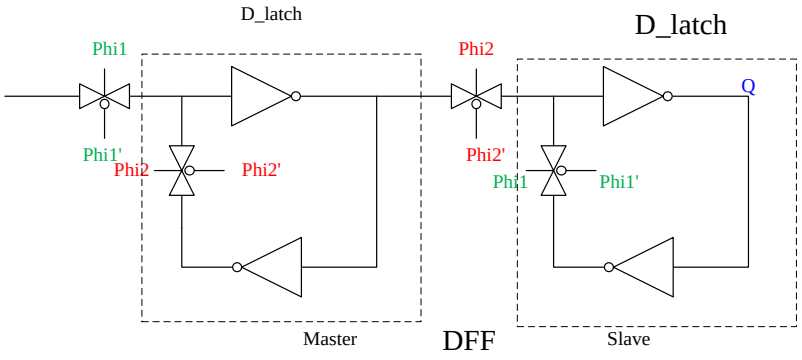
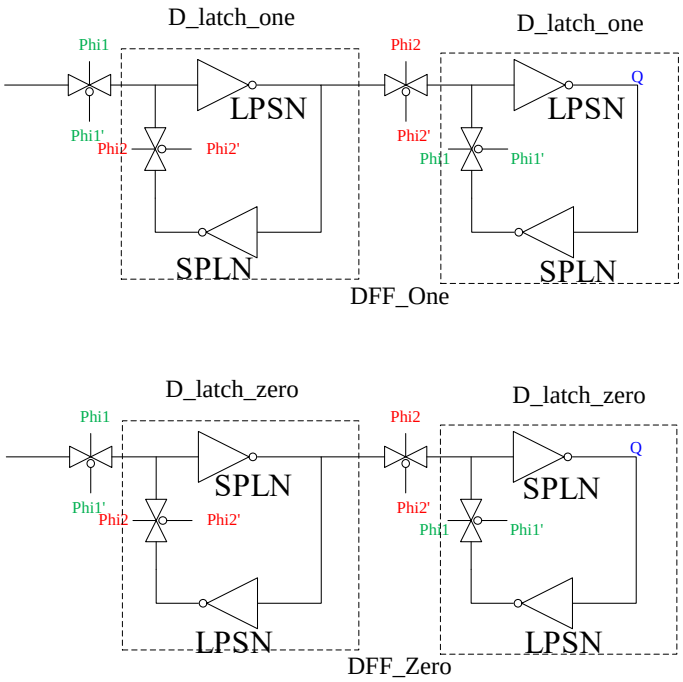


Figure 5-6 The transmission gate-based D flip-flop circuit

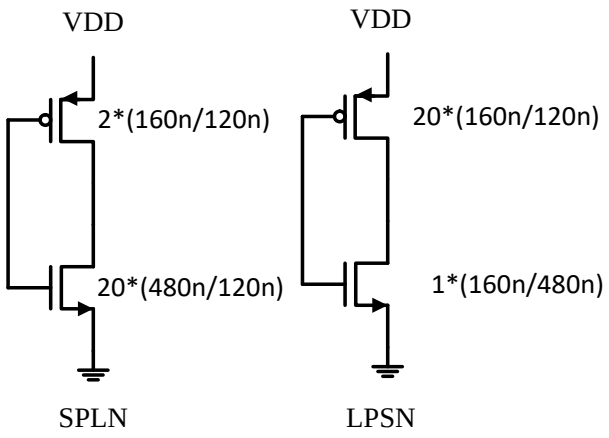
5.1.3 Comma sequence and random unique sequence

The shift register based PUF circuit is designed to have 84 DFFs in total connected together in a loop. Once the supply is set to 0.6V, the circuit will generate an 84-bit sequence cyclically. There are 64 random bits' generation DFFs, and an extra 20 Comma bits' generation DFFs. The 20 "Comma" in the loop is used to define the head of the 64-bit authentication sequence.

To have a large offset and make each bit robust to noise variations, minimum sized transistors are used in the random bits generation DFFs. In the 20 Comma bits DFFS, specially sized inverters in Figure 5-7 (c) are used to build the latch to have a predetermined state as shown in Figure 5-7(a) and (b). In Figure 5-7(a) and (b), the upper inverter and the lower inverter in the latches are switched to have latch cell with different predetermined state. As shown in Figure 5-8 (a) and (b), while the supply is ramping up, the state of each latch cell in the DFFs is predetermined to be 1 or 0.

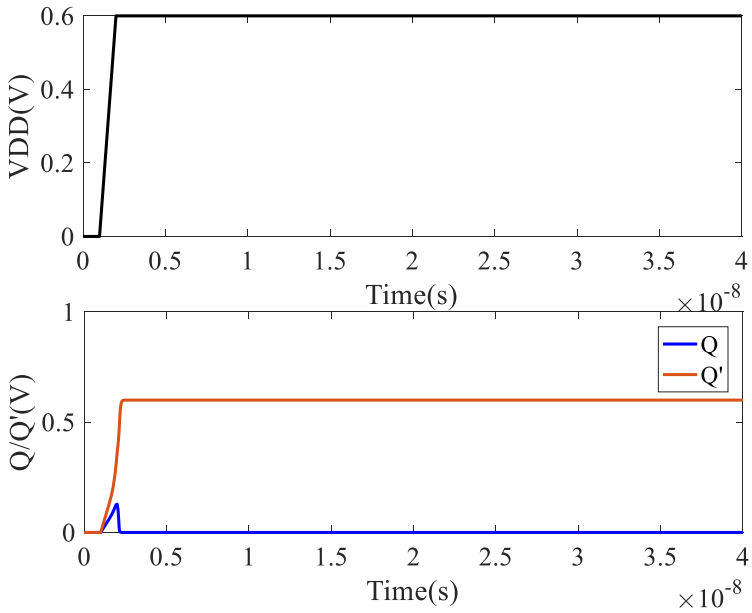


(a)

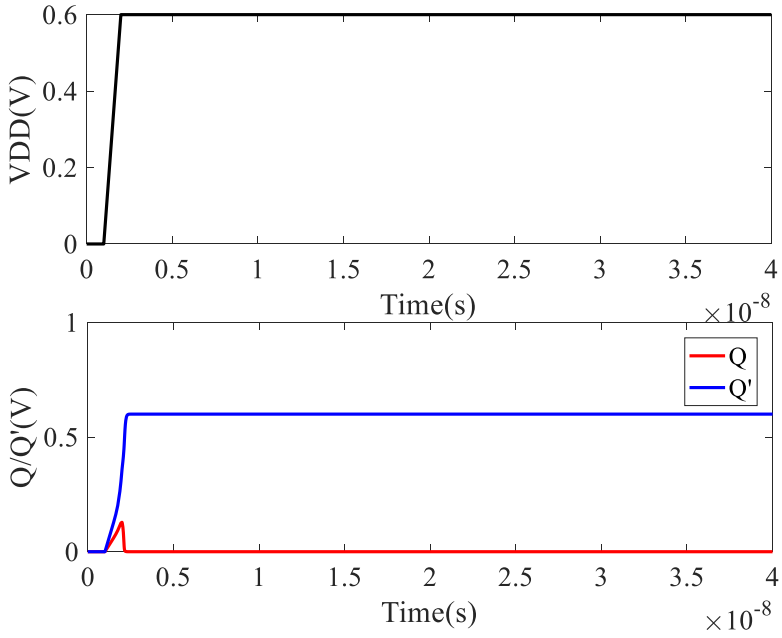


(b)

Figure 5-7 The DFF's with predetermined offset; (a) DFF-zero is a DFF with initial condition as zero; DFF-one is a DFF with initial condition as one;(b) the two inverters in DFF-zero and DFF-one



(a)



(b)

Figure 5-8 Transient response during supply ramping up of the predetermined latches;(a) response of latch_one; (b) response of latch_zero.

However, the random D flip-flop circuit shown in Figure 5-7, generating one or zero is not only determined by the offset in the latch as discuss above, but also determined by the clock signals. With the clock signals shown in Figure 5-9, if the DFF is powered up with clock phases same as at 't1', the initial state at 'Q' is determined by the slave latch; if it is powered up with clock phase same as at 't2', the initial state at 'Q' is determined by the left side latch but with an inversion bit; if it is turned on with clock phase same as at 't3', the two loops in the DFF are both open and the initial state cannot be predicted. Thus, to have the 'Comma' bits with a good control and be robust, the clock phases need to under control when the shift registrar based PUF circuit is powered up. In this design, the initial state determined by the slave latch are chosen to generate the 'Comma' bit, so the clock signals are designed

to stay as same phase as at ‘t1’ when the PUF circuit is turned on, which will be discussed in next session.

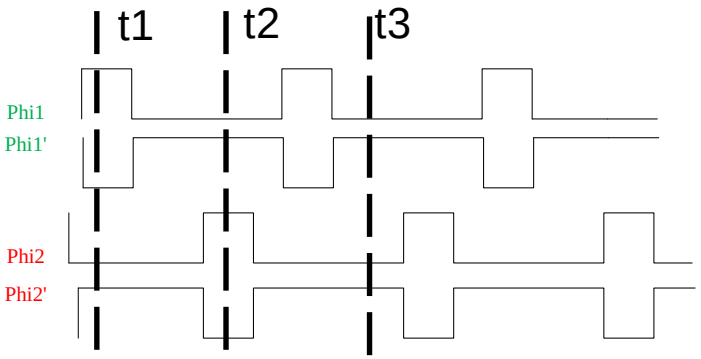


Figure 5-9 Two phase non-overlapping clock signals

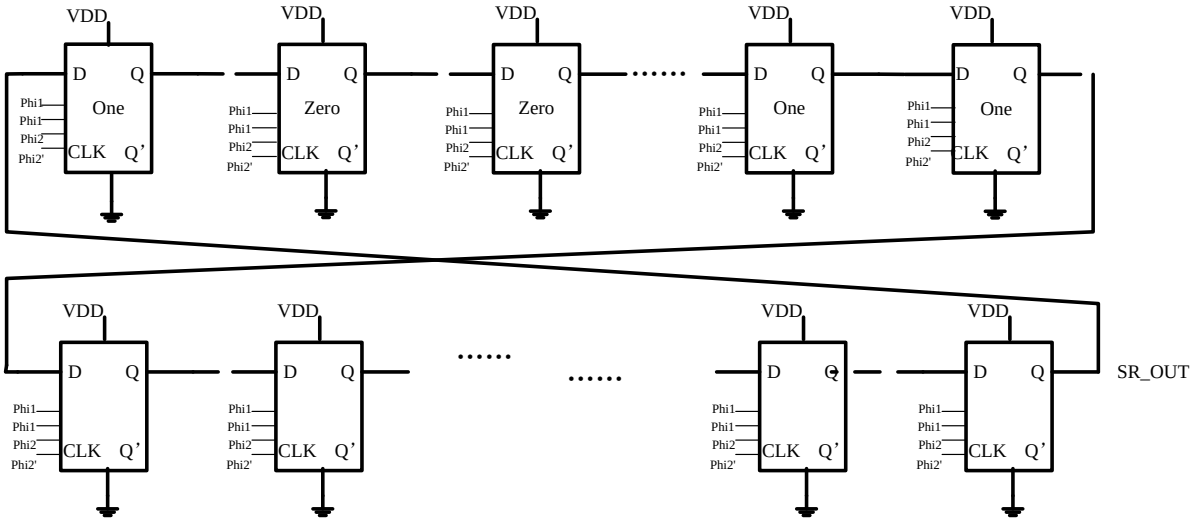


Figure 5-10 The shift register based PUF circuit

The 20-bit ‘comma’ can be any combination of ‘0’ and ‘1’. The only concern is that it should not be symmetric from the head to the tail. In this implementation, the comma is chosen as ‘1 0 0 1 0 1 0 1 0 1 0 0 1 1 0 0 1 0 1 1’. After this sequence, it starts the 64-bit unique authentication sequence. The whole shift register based PUF circuit diagram is shown in Figure 5-10.

5.1.4 Clock generation circuit

The built-in clock generation circuit is based on a three-stage ring oscillator circuit and three stage binary counter circuit. A simplified schematic showing the implementation of the clock circuit is in Figure 5-11.

The ring oscillator circuit generates a periodic sinewave signal, then two buffers are added to reshape the signal to a pulse wave. The transient response of the ring oscillator circuit and the reshaped signal are shown in Figure 5-12. To generate a 1MHz clock signal, three DFF's are used to make the clock frequency 8 times slower without requiring large transistors in the ring oscillator circuit. When the PMOS switch in Figure 5-1 is turned on, the clock circuit is powered and 1MHz clock signal is generated.

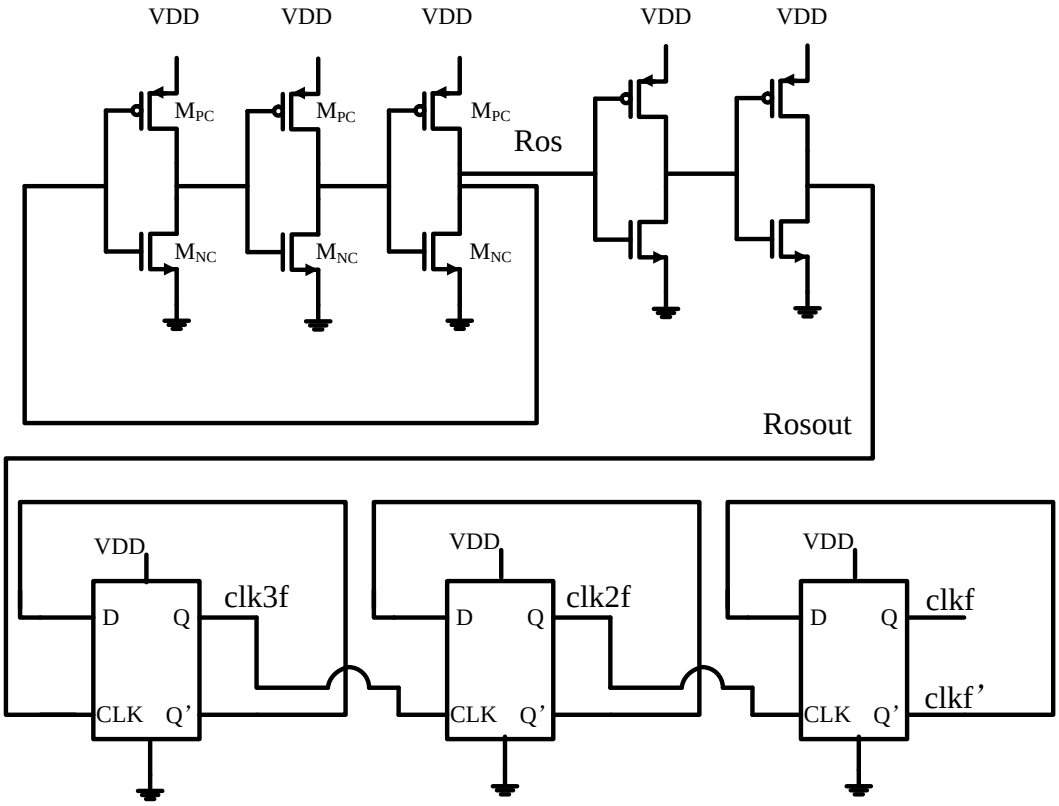


Figure 5-11 Ring oscillator-based clock generation circuits

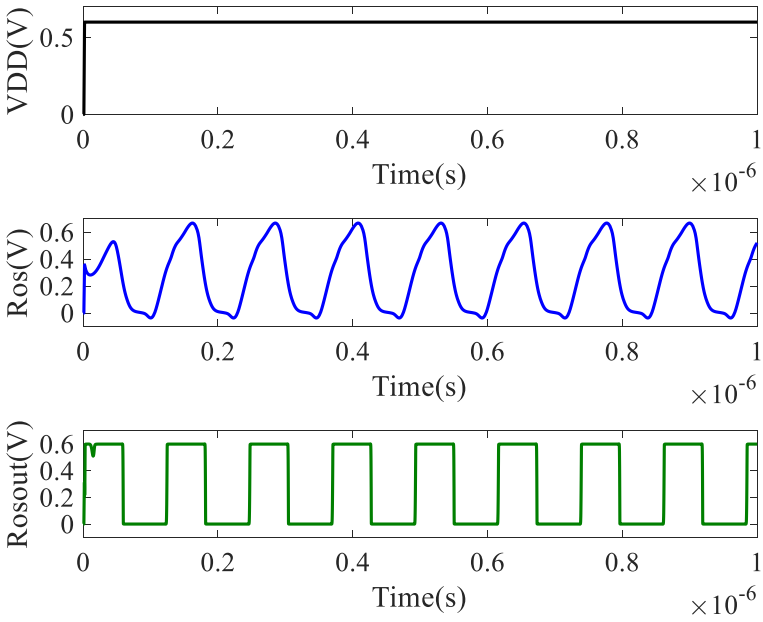


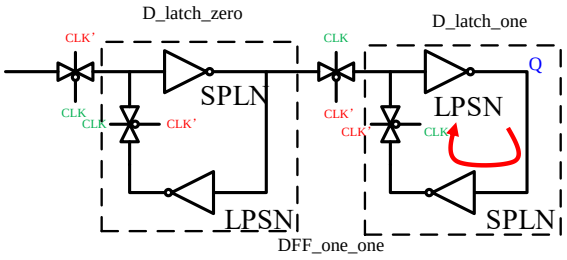
Figure 5-12 Transient response of the ring oscillator

The binary counter is also built with transition gate based DFFs. However, in the three binary counter architecture, the 'CLK'' is generated internally and locally, the overlapping between 'CLK' and 'CLK'' is only around 10ps, then the issue to have all switches on will not be a problem to change the operation of the circuit. Thus, in the frequency divider circuit, only 'CLK' and 'CLK'' are used, as shown in Figure 5-13.

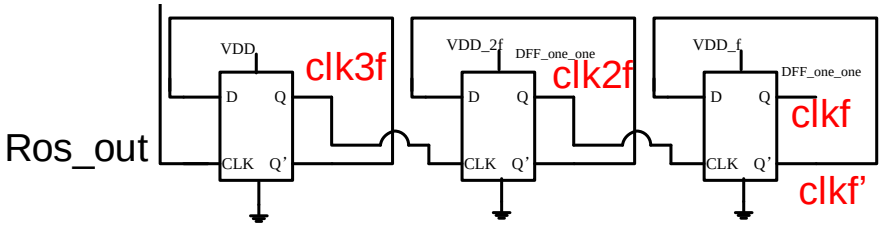
The D flip-flop circuit shown in Figure 5-7 generating one or zero is determined by the offset in the circuit as discuss above. But it is also determined by the clock signals. To make sure the initial state on the DFFs is determined by the slave latch cell, the clock signals should have the same clock phase as at 't1' in Figure 5-9 when the PUF circuit is turned on.

To meet this requirement, the second and third DFFs in the frequency divider is designed with the circuit shown in Figure 5-13(a), constructing the frequency divider as in Figure 5-13(b). The circuit named 'DFF_one_one' includes a 'D_latch_zero' as the master

latch and a ‘D_latch_one’ as the slave latch. At the moment when the circuit is turning on at t=0, no matter the slave loop or the master loop is closed first, the state at node Q is set as ‘1’. As shown in Figure 5-14 (a), if at the moment the second D_flip_flop turning on, signal at ‘clk3f’ is low, then the slave latch in the second D_flip_flop of the frequency divider is closed and ‘clk2f’ will start from high. Otherwise, as shown in Figure 5-14 (b), the signal at ‘clk3f’ is high, then the master latch in the second D_flip_flop is closed. ‘clk2f’ will be determined by the master latch. Since the master latch is latch zero, but after one inversion, ‘clk2f’ will be ‘high’ ,too. With a Q at ‘clk2f’ is ‘1’ in all conditions, the third DFF in the frequency divider will always have the slave latch on first and also generate ‘1’ at ‘clkf’ the moment when the supply is turning on. The ‘VDD_2f’ and ‘VDD_f’ are several nanoseconds delayed respectively by ‘VDD’ on the first DFF, to guarantee the clock ready earlier than the circuit powered up.

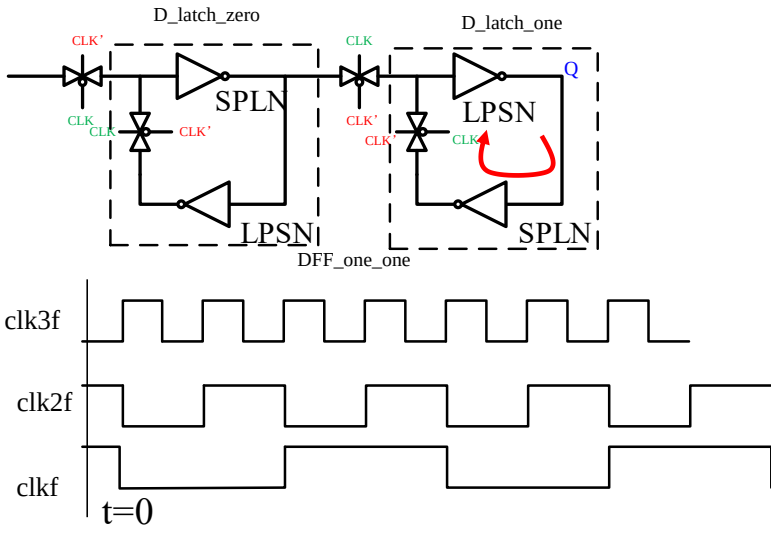


(a)

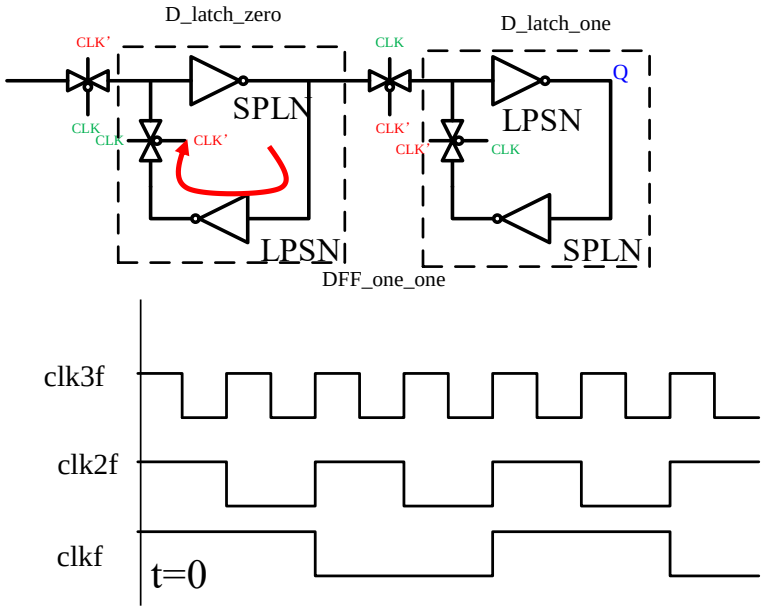


(b)

Figure 5-13 The second and third DFF design in the frequency divider;(a) The DFF_one_one circuit; (b) The frequency divider



(a)



(b)

Figure 5-14 The operation of the frequency divider with DFF_one_one;(a) The slave latch of DFF_one_one is on when circuit is turning on;(b) The master latch is on when the circuit is turning on.

With signals generated at ‘clk2f’, ‘clkf’’, and ‘clkf ’, the two-phase nonoverlapping clocks can be generated by the circuit shown in Figure 5-15. It will guarantee the slave latch in the PUF/shift register circuit will be closed first when the circuit is turning on.

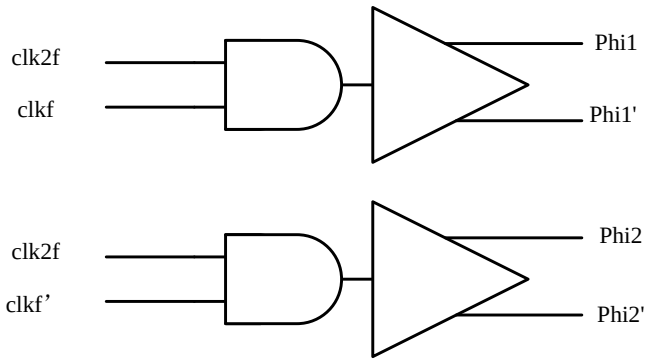


Figure 5-15 Nonoverlapping clock generation circuit

5.2 Simulation results

The under-circuit was designed in an IBM 0.13um process with a normal supply voltage of 1.2V. The circuit has been simulated using Monte Carlo transient tools in Spectre to verify its operation. Two transient simulation results of the shift register that show one cycle of the 20-bit comma and the first 15 bits of the random sequence are shown in Figure 5-16. The date sequences in all the simulation results have the same 20-bit ‘Comma’ sequences, but with different and unique random sequences.

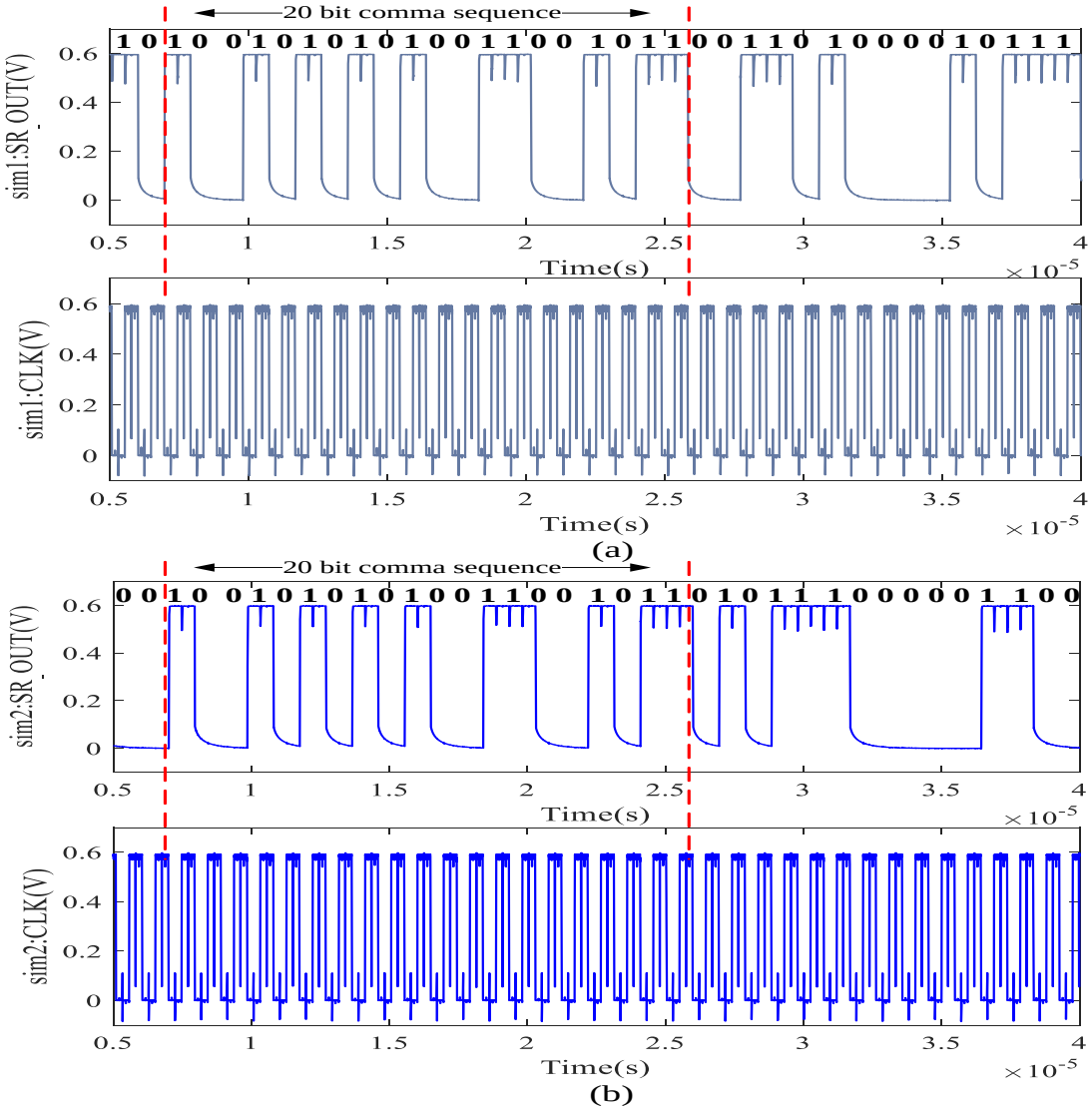


Figure 5-16 Parts of two simulation results

5.3 Statistical analysis

5.3.1 Distribution of latch state

As exploited in this paper, the physical mismatches on the minimum sized inverters determine the initial state when the latch turns on. However, it is not easy to analyze the distribution of the latch state directly, because the state is determined during the supply ramping up period. At the moment when the state is determined, the operation of transistors is uncertain.

The state in another structure shown in Figure 5-17 (a) can be analyzed. When 0<t<t1, the circuit are two separated self-biased inverters as shown in Figure 5-17(b). The voltage at node B and node A are the tripping points of the two inverters'. When t=t1, the inverter's gate capacitor will maintain the same voltage as 0<t<t1. When t>t1, the circuit is just the latch cell used in our PUF circuit. The voltage at node B and node A are the state of the latch cell and determined by the difference of the two inverter's tripping point.

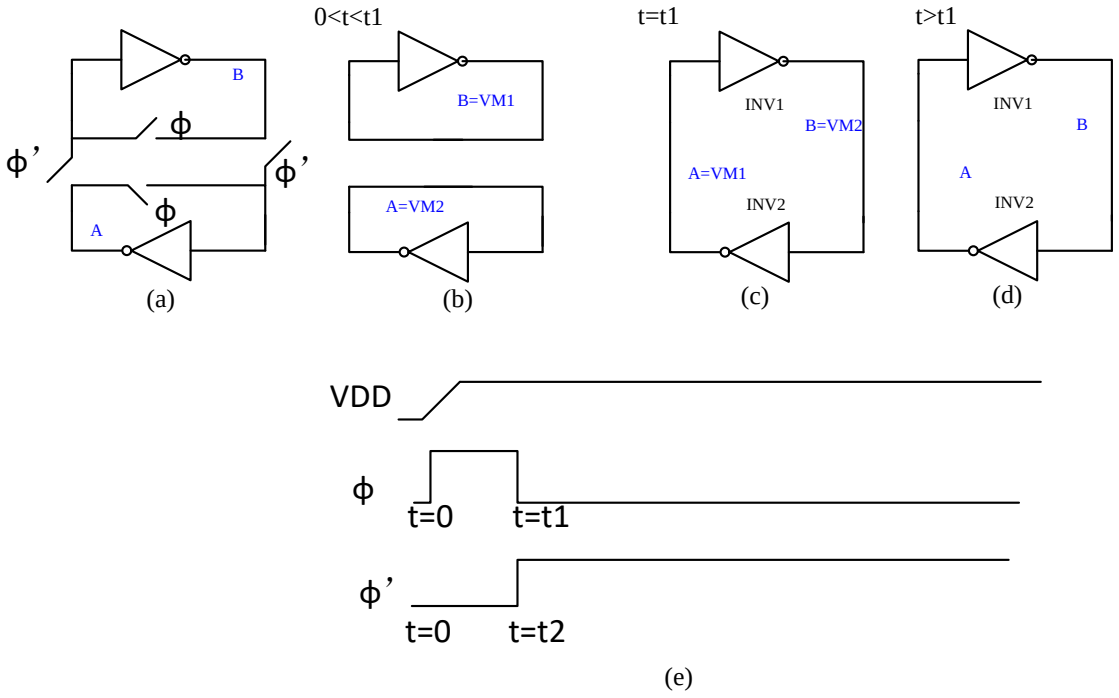


Figure 5-17 A circuit combined with two inverters and operating at two phases

If VM1 >VM2,

When t>t1, the signal at node B will start to increase because of the signal at node A is VM1; at the meantime, the signal at node A starts to decrease because of the signal at node B is VM2. Thus, the positive feedback loop in this latch cell will speed up this process keeping signal at node B increased to VDD, and signal at node A decreased to Gnd.

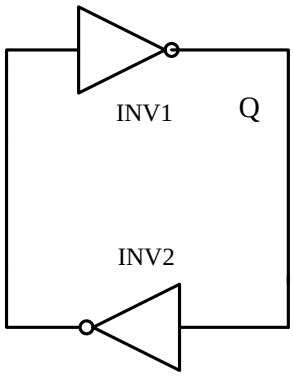
If VM1<VM2,

An inverse process will occur. Signal at node B will be Gnd and signal at node A will be VDD.

If VM1=VM2=VM,

Signal at node B and node A will always maintain as VM if no noise present.

Without noise consideration, verified by 10 simulations, same state can be achieved as the analysis above in the circuit show in Figure 5-18 which is the latch cell used in our PUF circuit. Thus, we assume the state in the two circuits have the same distribution characteristics. Thus the state Q on the latch in Figure 5-18 can be formulated as a function of the two inverters' tripping points VM as analysis on circuit of Figure 5-18.



$$Q = \begin{cases} 1 & VM1-VM2>0 \\ VM & VM1=VM2=VM \\ 0 & VM1-VM2<0 \end{cases}$$

Figure 5-18 Latch cell and the state of Q

Define $Voffset = V_{M1} - V_{M2}$, (5-1)

Thus, the distribution of Q can be calculated by the distribution of 'Voffset'.

At t=t1, assuming both PMOS and NMOS transistors are in the saturation region and conducting the same amount of current. The tripping point of the inverter can be calculated as Equations (5-2). With randomness analysis, the distribution of 'Voffset' can be calculated by Equations (5-3) to (5-14).

$$V_M = \frac{VDD + V_{Tp} + V_{Tn}\sqrt{\frac{\beta_n}{\beta_p}}}{1+\sqrt{\frac{\beta_n}{\beta_p}}} \tag{5-2}$$

Define, $\sqrt{\frac{\beta_n}{\beta_p}} = a, a = a_N + a_R,$

$$V_M \approx \frac{VDD + V_{TpN} + V_{TnN}a_N}{1+a_N} + \frac{V_{TpR}}{1+a_N} + \frac{a_N V_{TnR}}{1+a_N} + \frac{V_{TnN} - VDD - V_{TpN}}{(1+a_N)^2}a_R \tag{5-3}$$

$$V_{os} = V_M - V_{MN} \tag{5-4}$$

$$V_{os} \approx \frac{V_{TpR}}{1+a_N} + \frac{a_N V_{TnR}}{1+a_N} + \frac{V_{TnN} - VDD - V_{TpN}}{(1+a_N)^2}a_R \tag{5-5}$$

$$\delta^2_{os} \approx \frac{\delta^2_{V_{Tp}}}{(1+a_N)^2} + (\frac{a_N}{1+a_N})^2\delta^2_{V_{Tn}} + \frac{(V_{TnN} - VDD - V_{TpN})^2}{(1+a_N)^4}\delta^2_{aR} \tag{5-6}$$

$$a_R = \frac{1}{2}\sqrt{\frac{\mu_{nN}C_{oxnN}W_{nN}L_{pN}}{\mu_{pN}C_{oxpN}W_{pN}L_{nN}}}\left\{\frac{\mu_{nR}}{\mu_{nN}} + \frac{C_{oxnR}}{C_{oxnN}} + \frac{W_{nR}}{W_{nN}} + \frac{L_{pR}}{L_{pN}} - \frac{\mu_{pR}}{\mu_{pN}} - \frac{C_{oxpR}}{C_{oxpN}} - \frac{W_{pR}}{W_{pN}} - \frac{L_{nR}}{L_{nN}}\right\} \tag{5-7}$$

$$\delta_{a_R}^2 \approx \frac{1}{4}\frac{\mu_{nN}C_{oxnN}W_{nN}L_{pN}}{\mu_{pN}C_{oxpN}W_{pN}L_{nN}}\left\{\delta^2_{\frac{\mu_{nR}}{\mu_{nN}}} + \delta^2_{\frac{C_{oxnR}}{C_{oxnN}}} + \delta^2_{\frac{W_{nR}}{W_{nN}}} + \delta^2_{\frac{L_{pR}}{L_{pN}}} + \delta^2_{\frac{\mu_{pR}}{\mu_{pN}}} + \delta^2_{\frac{C_{oxpR}}{C_{oxpN}}} + \delta^2_{\frac{W_{pR}}{W_{pN}}} + \delta^2_{\frac{L_{nR}}{L_{nN}}}\right\} \tag{5-8}$$

Thus,

$$\delta^2_{os} \approx \frac{\delta^2_{V_{Tp}}}{(1+a_N)^2} + (\frac{a_N}{1+a_N})^2\delta^2_{V_{Tn}} + \frac{(V_{TnN} - VDD - V_{TpN})^2}{(1+a_N)^4}\frac{1}{4}a_N^2\left\{\delta^2_{\frac{\mu_{nR}}{\mu_{nN}}} + \delta^2_{\frac{C_{oxnR}}{C_{oxnN}}} + \delta^2_{\frac{W_{nR}}{W_{nN}}} + \delta^2_{\frac{L_{pR}}{L_{pN}}} + \delta^2_{\frac{\mu_{pR}}{\mu_{pN}}} + \delta^2_{\frac{C_{oxpR}}{C_{oxpN}}} + \delta^2_{\frac{W_{pR}}{W_{pN}}} + \delta^2_{\frac{L_{nR}}{L_{nN}}}\right\} \tag{5-9}$$

Assuming, the threshold voltage effects dominate the offset.

In this design, $a = \sqrt{\frac{\beta_n}{\beta_p}} = \sqrt{\frac{\mu_n C_{oxn} W_n L_p}{\mu_p C_{oxp} W_p L_n}} \approx 1$ (5-10)

Thus, $\delta^2_{os} \approx \frac{1}{4}\frac{A_{VTp0}^2}{W_{pN}L_{pN}} + \frac{1}{4}\frac{A_{VTn0}^2}{W_{nN}L_{nN}} = \frac{1}{4}\frac{8.1\times 8.1}{3\times 160\times 120} + \frac{1}{4}\frac{13.5\times 13.5}{160\times 120} = 0.00266V$ (5-11)

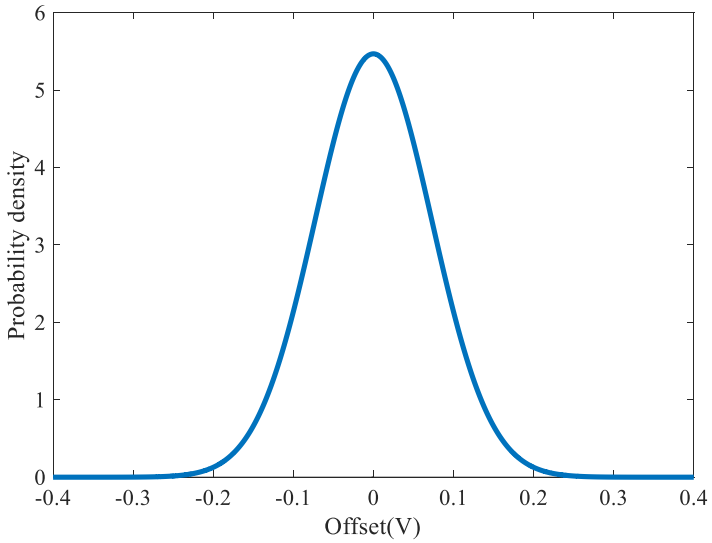
In the latch cell, the two inverters' tripping point have the same distribution characteristics, and same normal value, thus,

$$Voffset = V_{M1} - V_{M2} = V_{os1} + V_{MN} - V_{os2} - V_{MN} = V_{os1} - V_{os2} \quad (5\text{-}12)$$

Assuming, the two inverters' offset are iid, $\delta^2_{V_{offset}} = 2\delta^2_{os}$ (5-13)

$$\delta_{V_{offset}} = 0.07296V \quad (5\text{-}14)$$

The distribution of 'Voffset' is plotted in Figure 5-19. Based on the distribution of 'Voffset', the distribution of 'Q' can be calculated. Q is a function of a binomial distribution and with a probability as 0.5.



$$Q = \begin{cases} 1 & Voffset<0 \quad P(1)=0.5 \\ VM & Voffset=0 \quad P(VM)=0 \\ 0 & Voffset>0 \quad P(0)=0.5 \end{cases}$$

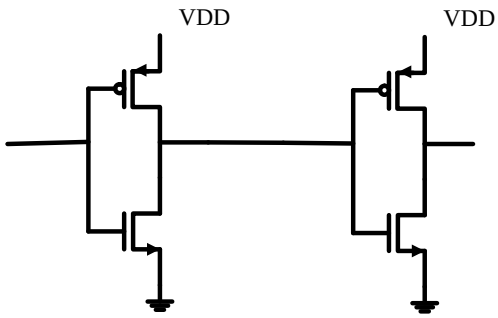
Figure 5-19 Distribution of 'Voffset'

5.3.2 Robustness of single bit

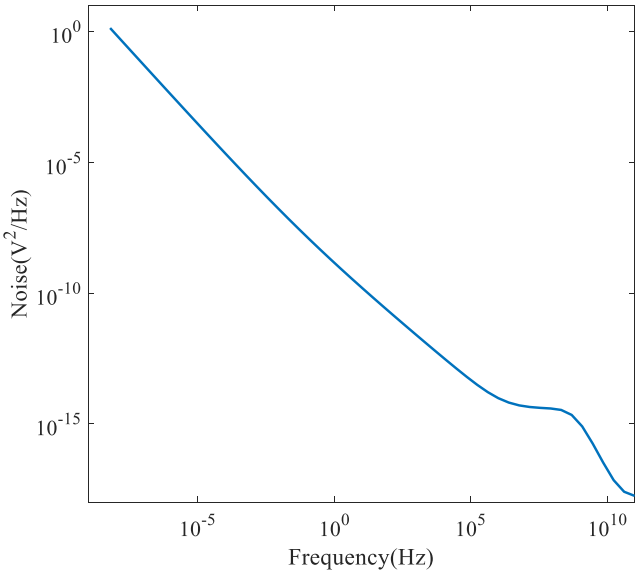
The distribution analysis of 'Q' is analyzed under the condition assumption that there is no noise present. However, if there is flicker and thermal noise existing in the circuit, the state of a device may vary from each test. Assuming a commercial device commonly used for 5 years, the V_{noise_rms} can be calculated by integrating the total noise. Noise simulation has been done on the minimum sized inverters on Figure 5-20 (a). As shown in Figure 5-20 (b), the thermal noise has been filtered out after 1GHz. Integrating the noise from 6.34×10^{-9} Hz to 1GHz, the total noise are calculated, as in Equation (5-15) and (5-16).

$$V_{n,noise}{}^{2} = 2.591\times10^{-6}V^{2} \tag{5-15}$$

$$V_{rms} = 1.6097mV \tag{5-16}$$



(a)



(b)

Figure 5-20 Inverter noise simulation results

In the real latch cell, if the noise is larger than the 'Voffset', the state of latch cell may be different in two tests, since the initial state will be impacted by noise; however, if the noise is much smaller than the 'Voffset', the state of latch cell will always be same in different tests since the initial state is dominated by 'Voffset'. With the distribution of 'Voffset' and noise, the robust bit and non-robust bit can be defined. Assuming the noise varies from -3Vrms to 3Vrms, the non-robust bit can be defined as when |offset| is lower than 3Vrms, while the robust bit is defined as when |offset| is larger than 3 V_{rms}. Thus the robust probability for one single bit can be calculated as Equation (5-17).

$$P(r) = 0.9471 \tag{5-17}$$

While the non-robust probability for one single bit is (5-18).

$$P(nr) = 0.0529 \tag{5-18}$$

5.3.3 Statistical analysis of the PUF circuits

If a code sequence from a customer' device has a hamming distance to a code in the database smaller than the tolerated hamming distance, the device is authenticated. Thus, to do authentication, a tolerated hamming distance need to be determined. In this section, a statistical analysis is done showing the strategy to determine the tolerated hamming distance.

5.3.3.1 Intra hamming distance

Intra hamming distance: Defined as the number of bits in a PUF response different from a repeated generation in the same device. It is a measure of the reproducibility of a PUF code generation.

In one PUF device, if bit 'i' is different in two different tests $D(i)^1 \neq D(i)^2$, the hamming distance increases by one.

The probability of a single bit is different at two tests in one PUF circuit is:

$$P(D(i)^1 \neq D(i)^2) = P_{iov} = 0.0529 \times \frac{1}{2} = 0.02645 \tag{5-19}$$

The probability of n bits different at the two tests in one device (or the probability of intra hamming distance as n) is:

$$P_{ihd} = \binom{64}{n} P_{iov}{}^{n} (1 - P_{iov})^{(64-n)} \tag{5-20}$$

The plot in Figure 5-21 is visually showing the Equation (5-20). There is a high probability that the intra hamming distance is less than 4. The intra hamming distance which is larger than 4 becomes very small. The probability for one PUF circuit to have at least 60 bits same in two different tests is 0.973. Thus, the proposed PUF circuit has a very good robust characteristic and there is a high probability to have at least 60 bits same in two

different tests. Based on this analysis, the tolerated hamming distance can be set as small as 4, which means when the hamming distance is no larger than 4 between the code from the customer device and the database, the device will be authenticated.

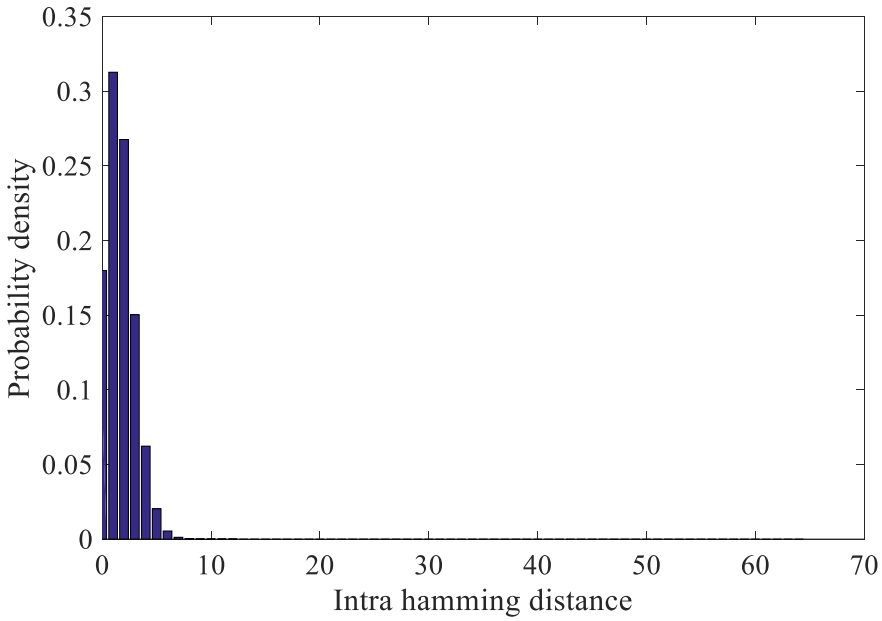


Figure 5-21The probability of different intra hamming distance in one device

5.3.3.2 Intra hamming distance

Inter hamming distance: Defined as the number of bits in a PUF response different from another PUF response in a different device. It is a measure of the uniqueness of an individual PUF circuit.

The probability function in Equation (5-21) plotted in Figure 5-22 shows the probability density of the different possible hamming distance in two different devices. As shown in Figure 5-22, the average inter hamming distance in this design is 32. The probability for having very low or very high inter hamming distance in two devices is small. If the tolerated hamming distance is set too large, the authentication's uniqueness will lose.

For example, if the tolerated hamming distance is set as 32, the probability to authenticate a device to another device is 0.5, which is too large.

$$P_{n\_ii'} = \binom{64}{n}\left(\frac{1}{2}\right)^{64} \tag{5-21}$$

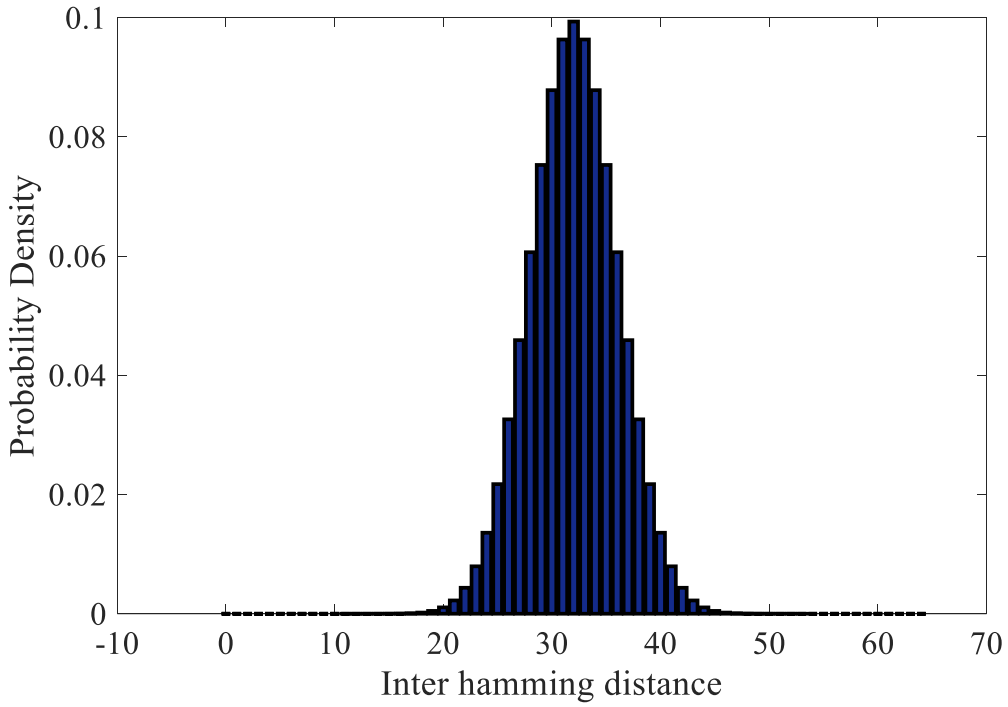


Figure 5-22 The probability of different inter hamming distance for two devices

To keep the uniqueness of the code sequence, the probability of the inter hamming distance in two devices smaller than the tolerated hamming distance which is defined as confused rate in the following section, should be small. Otherwise, it will be wrongly authenticated to another device. For different tolerated hamming distance N, the probability for the confused authentication in two devices is calculated by Equation (5-22) and plotted in Figure 5-23. The confused authentication means, the code sequences from the two devices are within the tolerated hamming distance, thus it cannot tell which code in the database comes from which device.

$$F_{confused}(n \le N) = \sum_{n=0}^{N} (\binom{64}{n})(\frac{1}{2})^{64} \quad (5\text{-}22)$$

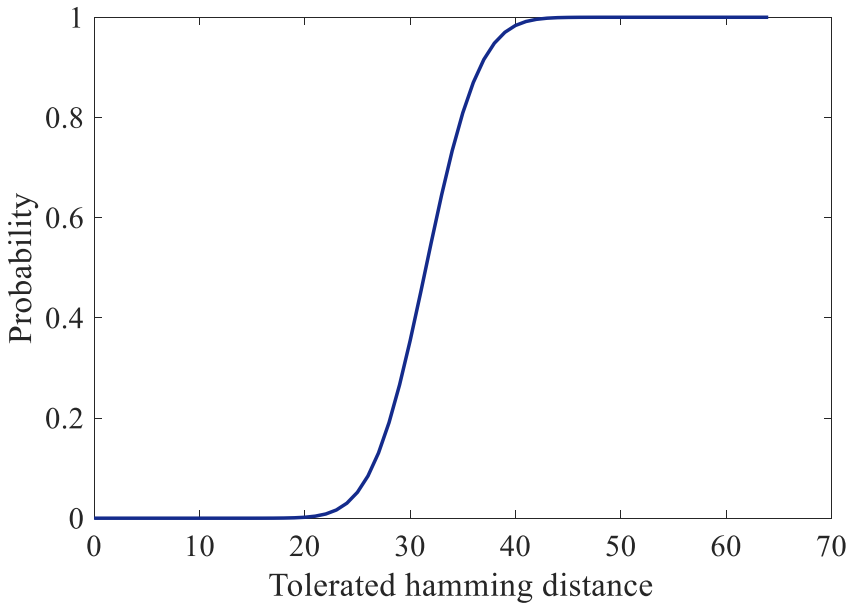


Figure 5-23 The rate for confused authentication for two devices

As shown in Figure 5-23, if the tolerated hamming distance is large, the rate to have confused authentication will be more close to 1. With a lower tolerated hamming distance, the rate to have confused authentication is smaller. In this project, if the tolerated hamming distance is set as 14, the confused rate is 3.5347×10^{-6} by Equation (5-23) which is very low. With the tolerated hamming distance as 14, if the 64-bit code from a customer's device has at least 50 bits same as a code in the database, the device is authenticated.

$$F_{confused}(n \le 14) = \sum_{n=0}^{14} (\binom{64}{n})(\frac{1}{2})^{64} \quad (5\text{-}23)$$

For two devices, with 14 as the tolerated hamming distance, the probability to have confused authentication is low. However, if the total number of products is large, the probability to have two devices with a hamming distance smaller than the tolerated hamming

distance will also increase. Assuming for one fixed sequence code from a device, the probability for another device to have at least 50 bits same as this fixed code is calculated by Equation (5-24).

$$P_{50bits}(n \le 14) = \sum_{n=0}^{4} \binom{64}{n} \times (\frac{1}{2})^{64} = 3.5347e-6 \quad (5\text{-}24)$$

Among the total products of which the number is 'M', the probability to have more than one device with at least 50 bits same as the code sequence from a device at different 'M' is calculated by Equation (5-25) and plotted in Figure 5-24.

$$F_{confused\_in\_M} = 1-(1-P_{50bits})^{M-1} \quad (5\text{-}25)$$

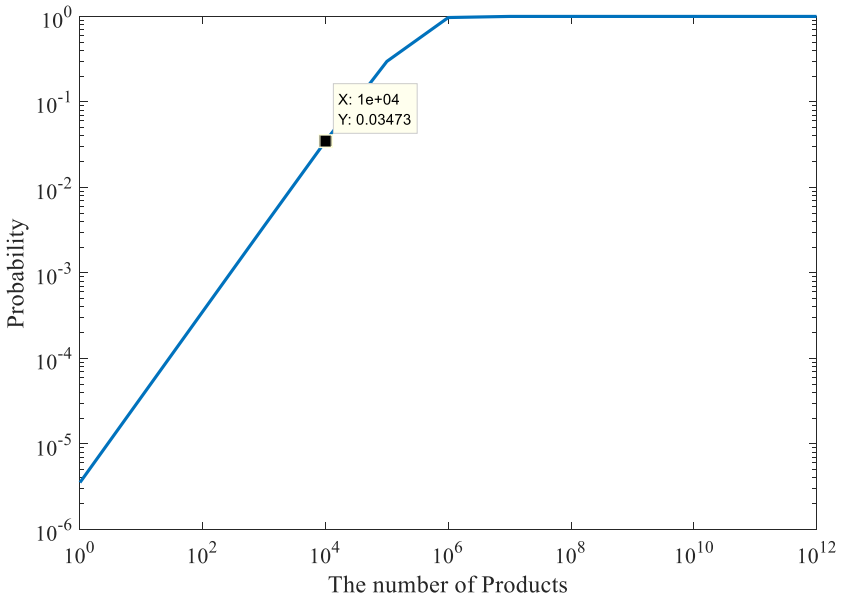


Figure 5-24 The number of products VS the rate of confused authentication with tolerated hamming distance as 14

As shown in Figure 5-24, the rate of having at least two confused authentication devices will increase as the number of products increases. If the tolerated hamming distance is 14 as shown in Figure 5-24, with the total number of products as ten thousands, the rate of confused authentication is 0.03.

Different tolerated hamming distance will result different functions of the confused rate and the total number of products. To generate large number of devices, and have a low rate of confused authentication, the tolerated hamming distance need to be set smaller. For example, if the hamming distance is set as 8, the probability of one PUF with at least 56 bits same as another device is much smaller, shown in Equation (5-26).

$$P_{56bits}(n \le 8) = \sum_{n=0}^{8} \binom{64}{n} \times \left(\frac{1}{2}\right)^{64} = 2.7813 \times 10^{-10} \tag{5-26}$$

With 8 as the tolerated hamming distance, the number of products VS the probability of having at least two products with at least 56 bits same in the total devices is plotted in Figure 5-25 and expressed by Equation (5-27).

$$F_{confused\_in\_M} = 1 - (1 - P_{56bits})^{M-1} \tag{5-27}$$

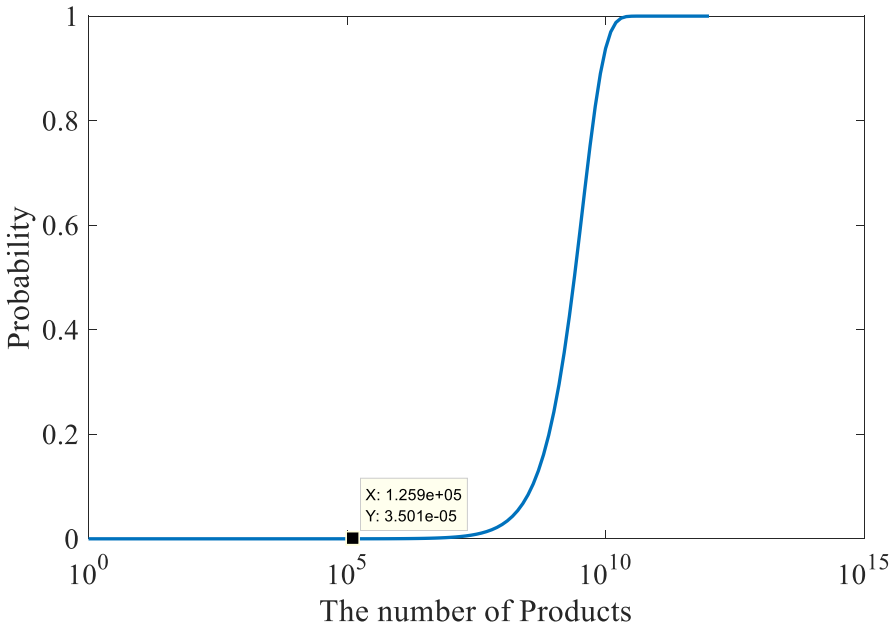


Figure 5-25 The number of products VS the rate of confused authentication with tolerated hamming distance as 8

As shown in Figure 5-25, when the tolerated hamming distance is 8, the rate of confused authentication comes to very low even when the total number of products is over hundreds thousand.

As analysis above, the tolerated hamming distance can be set based on the inter hamming distance and the intra hamming distance. With the inter hamming distance analysis, it's known that the tolerated hamming distance should be set larger than 4 to lower the probability of missing authentication to a right device. With the intra hamming distance analysis, it's known that the tolerated hamming distance should be chosen based on the number of products and the rate of confused authentication. If the number of products is around hundred thousand, the tolerated hamming distance can be chosen as large as 8 but still with a very a good uniqueness rate for authentication. Actually, in real case, a very good uniqueness may not be an important concern. Even there are some confused devices, compared to the earrings, the loss to throw away some confused devices is too low. Thus, a little bit higher tolerated hamming distance may also be used depending on the financial analysis.

CHAPTER 6. CONCLUSION

In conclusion, the research work in this dissertation is focused on analog hardware security and hardware authentication. A type of power/area/architecture/ signature transparent analog hardware Trojan is analyzed. Example circuits showing the PAAST characteristics are given. Detecting methods focusing on Trojan in static and dynamic analog circuits are proposed. A PUF circuit built with sub threshold under circuit is designed for circuit authentication. The proposed circuit architecture for authentication doesn't need any extra pins besides the pins necessary for the original IC.

In Chapter 2, it shows example circuits with Trojan states served by extra operating points or modes. These Trojan can exist in both static circuit and dynamic circuit; they can be in the frequency domain, phase domain or voltage amplitude domain; and they are also Power/Area/Architecture and Signature Transparent. Hence, they are extremely challenging to detect with state of art simulation and verification tools or existing hardware Trojan detection methods even if a complete and accurate disclosure of the circuit is given. These Trojans can be readily embedded in some of the most basic analog and mixed-signal circuit structures. Irrespective of whether PAAST Trojans are accidentally or maliciously inserted or Triggered, the presence of these Trojans can cause disastrous results. Additionally, three temperature signatures of multiple equilibriums in inverse Widlar circuit is observed. Base on the type 2 signature, a tiny temperature trigger circuit is designed.

In Chapter 3, due to the temperature sensitive characteristics, a bi-directional temperature sweeping method detecting the existence of undesired operating points is proposed. By doing a bi-directional temperature sweeping simulation, a hysteresis window can be observed if at low temperature and high temperature the circuit has worked at two

different operating points. Application of this method on many different circuits has shown that it works well on almost all the circuits, except those with isolated equilibrium points in the temperature domain. But if combined with other methods, the temperature sweeping method is still efficient to speed up the verification process. Additionally, a one-dimensional initial condition scanning method for identifying the presence or absence of Trojan stationary dynamic modes of operation in nonlinear dynamic circuits was introduced for dynamic circuits. It is based upon a sequence of transient simulations whereby the initial conditions for each transient simulation are elements of a finite scan set. By scanning the initial conditions, at least one point in the domain of convergence for each orbit of the circuit can be reached. This method works efficient on second order dynamic circuits and it can also detect the existence of Trojan modes in higher order systems.

In Chapter 4, it introduces a side-channel trigger mechanism which can be used to trigger analog circuits with PAAST Trojans into an undesired redundant stationary mode during its normal operation. Since these side-channel triggers doesn't need any extra circuit inserted to the original system or any extra interconnects among the original blocks, it won't consume more power, take more area, or have any circuit architecture modification, current signature vaiation in the supply bus or delay variation in the timing path. The trigger mechanism is also PAAST. Measurement results of two dynamic circuits with multiple operating modes are also given for demonstration of PAAST Trojans' existence.

In Chapter 5, a shift register PUF based undercircuit which can operate at half supply to generate a unique key for IC authentication purposes has been proposed. It has no interaction with the COTS IC during normal operation. By dual-purposing three pins of the original IC, it requires no extra pins. When the circuit is implemented underneath existing

bonding PADs, it consumes no extra die area. Additionally, statistical analysis has been done to show the strategy to determine the tolerated hamming distance.

REFERENCES

[1] H. Salmani, M. Tehranipoor, and J. Plusquellic. “A novel technique for improving hardware trojan detection and reducing trojan activation time,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vo. 20(1), pp. 112-125

[2] M. Li, A. Davoodi, and M. Tehranipoor. "A sensor-assisted self-authentication framework for hardware trojan detection." In Proceedings of the Conference on Design, Automation and Test in Europe, pp. 1331-1336. EDA Consortium, 2012

[3] M. Tehranipoor, and F. Koushanfar. "A survey of hardware Trojan taxonomy and detection." IEEE Design and Test of Computers 27,vo. no. 1 (2010), pp. 10-25

[4] X, Zhang, and M. Tehranipoor. "RON: An on-chip ring oscillator network for hardware Trojan detection." In 2011 Design, Automation & Test in Europe, pp. 1-6. IEEE, 2011

[5] K. Xiao, D. Forte, and M. Tehranipoor, “A novel built-in self-authentication technique to prevent inserting hardware Trojans,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 33(12), pp.1778-1791.2014

[6] Y. Wang, Q. Wang, D. Chen, and R. L. Geiger. "Hardware Trojan state detection for analog circuits and systems." In NAECON 2014-IEEE National Aerospace and Electronics Conference, pp. 364-367. 2014.

[7] Q. Wang, R. L. Geiger, and D. Chen. "Hardware Trojans embedded in the dynamic operation of analog and mixed-signal circuits." In 2015 National Aerospace and Electronics Conference (NAECON), pp. 155-158, 2015.

[8] U. Guin, K Huang, D DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris. "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain." *Proceedings of the IEEE* 102, no. 8 (2014): 1207-1228.

[9] N. Kae-Nune and S. Pesseguier, ‘‘Qualification and testing process to implement anti-counterfeiting technologies into IC packages,’’ Proc. Eur. Conf. on Design Automation and Test, pp. 1131–1136, 2013.

[10] “2016 Top Markets Report Semiconductors and Semiconductor Manufacturing Equipment Sector Snapshot”, International Trade Administration, US Department of Commerce.

[11] Oral Testimony of SIA President Brian Toohey, Senate Armed Services Committee Hearing on Counterfeit Electronic Parts in the Department of Defense’s Supply Chain, November 8, 2011.

[12] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, ‘‘Design and implementation of PUF-Based ‘unclonable’RFID ICs for anti-counterfeiting and

security applications,'' in Proc. IEEE Int. Conf. RFID, May 2008, pp. 58–64.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[13] C. Herder, M. Yu, F. Koushanfar, S. Devadas, "Physical unclonable functions and applications:A tutorial," Proc. IEEE, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[14] G. Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In Proceedings of the44th Design Automation Conference, pages 9–14. IEEE, 2007.

[15] A. Das, Kocabaş, Ü., Sadeghi, A.-R., Verbauwhede, I.: PUF-based secure test wrapper design for cryptographic SoC testing. In: Design, Automation & Test in Europe, DATE 2012, pp. 866–869 (March 2012)

[16] J. Li and J. Lach, ''At-Speed Delay Characterization for IC Authentication and Trojan Horse Detection,'' Proc.IEEE Int'l Workshop Hardware-Oriented Security and Trust (HOST 08), IEEE CS Press, 2008, pp. 8-14.

[17] C. G. Broyden,"A class of methods for solving nonlinear simultaneous equations." Mathematics of computation 19, no. 92 (1965), pp. 577-593.

[18] V. Kumar. "A Nonsmooth Exclusion Test for Finding All Solutions of Nonlinear Equations." PhD diss., Massachusetts Institute of Technology, 2007.

[19] C. D. Maranas, and C. A. Floudas. "Finding all solutions of nonlinearly constrained systems of equations." Journal of Global Optimization 7, no. 2 (1995), pp. 143-182.

[20] C. Grosan, and A. Abraham, "Multiple solutions for a system of nonlinear equations," International Journal of Innovative Computing, Information and Control, vo. 4(9), pp. 2161-2170, (2008).

[21] L. O. Chua, and A. Ushida. "A switching - parameter algorithm for finding multiple solutions of nonlinear resistive circuits." International Journal of Circuit Theory and Applications, vo. 4(3), pp. 215-239. (1976).

[22] B. G. Lee, A. N. Willson, "All two-transistor circuits possess at most three dc operating equilibrium points." In *Proc. 26th Midwest Symp. Circuits and Systems, Puebla, Mexico, 1983*, pp. 504-507. 1983.

[23] A. Ushida, Y. Yamagami, Y. Nishio, I. Kinouchi, and Y. Inoue. "An efficient algorithm for finding multiple DC solutions based on the SPICE-oriented Newton homotopy method." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 21, no. 3, PP. 337-348. 2002.

[24] L. B. Goldgeisser, and M. M. Green. "A method for automatically finding multiple operating points in nonlinear circuits." IEEE Transactions on Circuits and Systems I: Regular Papers, vo. 52, no. 4, pp. 776-784. (2005),

[25] Q. Wang, and R. L. Geiger. "Temperature signatures for performance assessment of circuits with undesired equilibrium states." Electronics Letters,vo. 51, no. 22, pp. 1756-1758. (2015).

[26] Y. Wang, D. J. Chen, and R. L. Geiger. "Effectiveness of circuit-level continuation methods for Trojan State Elimination verification." In 2013 IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 1043-1046, 2013.

[27] E.O. HWANG, "Microprocessor design principles and practices with VHDL," (2004).

[28] R.S. Chakraborty, S. Narasimhan, and S. Bhunia. "Hardware Trojan: Threats and emerging solutions." In High Level Design Validation and Test Workshop, 2009. HLDVT 2009. IEEE International, pp. 166-171.

[29] A. Reibiger, W. Mathis, T. Nähring, and L. Trajković. "Mathematical foundations of the TC-method for computing multiple DC-operating points." International Journal of Applied Electromagnetics and Mechanics 17, no. 1-3, pp. 169-191, (2003).

[30] L. B. Goldgeisser, and M. M. Green. "On the topology and number of operating points of MOSFET circuits." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 48, no. 2. pp. 218-221. (2001).

[31] Z. Liu, Y. Li, R. L. Geiger, and D. Chen. "Auto-identification of positive feedback loops in multi-state vulnerable circuits." IEEE, In VLSI Test Symposium (VTS), 2014 IEEE 32nd, pp. 1-5. 2014.

[32] Q. Wang, R. L. Geiger, and D. J. Chen. "Challenges and opportunities for determining presence of multiple equilibrium points with circuit simulators." In 2014 IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 406-409, 2014.

[33] X. Cao, Q. Wang, R. L. Geiger, and D. J. Chen. "A hardware Trojan embedded in the Inverse Widlar reference generator." In 2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 1-4. 2015.

[34] H. Banba, H. Shiga, A. Umezawa, T. Miyaba, T. Tanzawa, S. Atsumi, and K. Sakui. "A CMOS bandgap reference circuit with sub-1-V operation." *IEEE Journal of Solid-State Circuits* 34, no. 5, pp. 670-674. 1999.

[35] R. P. Sallen, and E. L. Key. A practical method of designing RC active filters. MIT Lincoln Laboratory, 1954.

[36] A. Fukuma and M. Matsubara, "Jump resonance criteria of nonlinear control systems." Automatic Control, IEEE Transactions on 11.4 (1966): 699-706.

[37] K. AONO, R. K. Shaga, and S. Chakrabartty. "Exploiting Jump Resonance hysteresis in silicon auditory front-ends for extracting speaker discriminative formant

trajectories," Biomedical Circuits and Systems, IEEE Transactions on. 7(4), pp. 389-400, 2013.

[38] C. D. Salthouse,and R. Sarpeshkar. "Jump resonance: a feedback viewpoint and adaptive circuit solution for low-power active analog filters." Circuits and Systems I: Regular Papers, IEEE Transactions on 53.8 (2006): 1712-1725.

[39] P. Allen, "A model for slew-induced distortion in single-amplifier active filters." *IEEE Transactions on Circuits and Systems* 25, no. 8 (1978): 565-572.

[40] Z. Bai, X. Zhou, and R. Mason. "A novel injection locked rotary traveling wave oscillator." In Circuits and Systems (ISCAS), 2014 IEEE International Symposium on, pp. 1768-1771.

[41] F. O'Mahony, C. P. Yue, M. A. Horowitz, and S. Wong. "A 10-GHz global clock distribution using coupled standing-wave oscillators." IEEE Journal of Solid-State Circuits 38, no. 11 (2003): 1813-1820.

[42] K. Takinami, and R. Walsworth. "Phase error calibration technique for rotary traveling wave oscillators." IEEE Journal of Solid-State Circuits 45, no. 11 (2010): 2433-2444.

[43] J. Roychowdhury, "Boolean computation using self-sustaining nonlinear oscillators." Proceedings of the IEEE 103, no. 11 (2015): 1958-1969.

[44] S. Li, I. Kipnisand M., Ismail, 2003. A 10-GHz CMOS quadrature LCVCO for multirate optical applications. IEEE Journal of Solid-State Circuits, 38(10), pp.1626-1634.

[45] H. Tong, S. Cheng, Y. Lo, A.I. Karsilayan, and J. Silva-Martinez. "An LC quadrature VCO using capacitive source degeneration coupling to eliminate bi-modal oscillation." IEEE Transactions on Circuits and Systems I: Regular Papers 59, no. 9 (2012): 1871-1879.

[46] S. Youn, J. Kim, and M. Horowitz. "Global convergence analysis of mixed-signal systems." In Proceedings of the 48th Design Automation Conference, pp. 498-503. ACM, 2011.

[47] S. Wei, and M. Potkonjak. "The undetectable and unprovable hardware trojan horse." In Proceedings of the 50th Annual Design Automation Conference, ACM. pp. 144-145. 2013.

[48] Y-T, Wang, D, Chen, and R.L, Geiger, "Practical methods for verifying removal of Trojan stable operating points." Circuits and Systems (ISCAS), 2013, pp. 2658-2661

[49] Q. Wang, R.L. Geiger, and D. Chen, (2015, May). A programmable temperature trigger circuit. In Circuits and Systems (ISCAS), 2015 IEEE International Symposium on (pp. 1070-1073). IEEE.

[50] D. E. Duarte, G. Taylor, K. L Wong, “Advanced thermal sensing circuit and test techniques used in a high performance 65nm processor,” In Low Power Electronics and Design (ISLPED), 2007 ACM/IEEE International Symposium on (pp. 304-309).

[51] C. Zhao, Y. T. Wang, D. Genzer, D. Chen, and R. Geiger, “A CMOS on-chip temperature sensor with− 0.21° C 0.17° C inaccuracy from− 20° C to 100° C,” In Circuits and Systems (ISCAS), 2013 IEEE International Symposium on (pp. 2621-2625).

[52] K. Souri, Y. Chae, and K. A. Makinwa, “A CMOS Temperature Sensor With a Voltage-Calibrated Inaccuracy of 0.15 C (3) From 55° C to 125° C”. Solid-State Circuits, IEEE Journal of, 48(1), 292-301.

[53] A. Bakker, “CMOS smart temperature sensors-an overview.” In Sensors, 2002. Proceedings of IEEE (Vol. 2, pp. 1423-1427).

[54] D. Brooks, and M. Martonosi, “Dynamic thermal management for high-performance microprocessors.” In High-Performance Computer Architecture, 2001. HPCA. The Seventh International Symposium on (pp. 171-182).

[55] B. L. Dokić, (1984, October). CMOS Schmitt triggers. In IEE Proceedings G (Electronic Circuits and Systems) (Vol. 131, No. 5, pp. 197-202). IET Digital Library.

[56] M. Li, A. Davoodi, and M. Tehranipoor, “A sensor-assisted self-authentication framework for hardware trojan detection”. In Proceedings of the Conference on Design, Automation and Test in Europe, pp. 1331-1336. EDA Consortium, 2012.

[57] M. Tehranipoor, and F. Koushanfar. "A survey of hardware Trojan taxonomy and detection." IEEE Design and Test of Computers 27,vo. no. 1 (2010), pp. 10-25.

[58] Y. Liu, K. Huang, and Y. Makris, "Hardware Trojan detection through golden chip-free statistical side-channel fingerprinting." Proceedings of the Design Automation Conference (DAC), pp. 1-6, 2014.

[59] Y. Wang, Z. Chen, R. L. Geiger, D. Chen, and S. Huang, “Performance verification of start-up circuits in reference generators.” In 2012 IEEE 55th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 518-521, 2012.

[60] K. Yamamura, and N. Tamura, “Finding all solutions of separable systems of piecewise-linear equations using integer programming,” Journal of Computational and Applied Mathematics Vol. 236, pp.2844–2852. 2012.

[61] S. Halgas, M. Tadeusiewicz, “Analysis of CMOS circuits having multiple DC operating points,” Przeglad Elektrotechniczny (Electrical Review), pp. 40-42, May 2011.

[62] R. Nielson, A. Willson, “A Fundamental Result Concerning the Topology of Transistor Circuits with Multiple Equilibria,” Proc. Of the IEEE, pp. 196-198, Feb. 1980.

[63] G. Gajani, A. Brambilla, and A. Premoli, “Numerical Determination of Possible Multiple DC Solutions of Nonlinear Circuits,” TCAS. pp.1074-1083, May 2008.

[64] R. Melville, L. Trajkovic, S. Fang, and L.T. Watson, “Artificial Parameter Homotopy Methods for the DC Operating Point Problem,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), pp. 861-877, June 1993.

[65] Li, You, and Degang Chen. "Efficient analog verification against Trojan states using divide and contraction method." IEEE, In Circuits and Systems (ISCAS), 2014 IEEE International Symposium on, pp. 281-284. 2014.

[66] M. M. Green, and A. N. Willson. "(Almost) half of any circuit's operating points are unstable." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 41, no. 4, pp.286-293. (1994)

[67] F. Fiori, and P. S. Crovetti. "A new compact temperature-compensated CMOS current reference." IEEE Transactions on Circuits and Systems II: Express Briefs 52, no. 11, pp. 724-728. (2005).

[68] J. He, C. Zhao, S-H. Lee, K. Peterson, R. Geiger, and D. Chen. "Highly linear very compact untrimmed on-chip temperature sensor with second and third order temperature compensation." IEEE, In Circuits and Systems (MWSCAS), 2010 53rd IEEE International Midwest Symposium on, pp. 288-291. 2010.

[69] J.-W. Lee, D. Lim, B. Gassend, G. E. Suh, M. V. Dijk, and S. Devadas. A technique to build a secret key in integrated circuits with identification and authentication applications. In Proceedings of the IEEE VLSI Circuits Symposium, June 2004.

[70] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, “A physically unclonable function with BER<10-8 for robust chip authentication usingoscillator collapse in 40 nm CMOS,” in Proc. 2015 IEEE Int. Solid State Circuits Conf., San Francisco, CA, USA, Feb. 2015, pp. 1–3.

[71] 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 58, no. 9 (2009): 1198-1210.