2016

Ultra-small low power temperature-to-digital converter and verification methods of analog circuit with Trojan states

Yen-Ting Wang
Iowa State University

Ultra-small low power temperature-to-digital converter and verification methods of analog circuit with Trojan states

by

Yen-Ting Wang

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Electrical Engineering

Program of Study Committee:
Randall Geiger, Major Professor
Degang Chen
Ayman Fayed
Sumit Chaudhary
William Meeker

Iowa State University

Ames, Iowa

2016

DEDICATION

To my Parents

TABLE OF CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

Page

NOMENCLATURE

CMOS	Complementary metal-oxide-semiconductor
BJT	Bipolar Junction Transistor
VLSI	Very-large-scale Integration
IC	Integrated Circuit
TSE	Trojan State Elimination
V_{TH}	Threshold voltage
PVT	Process/Voltage/Temperature

ACKNOWLEDGMENTS

I would like to thank my committee chair, Dr. Geiger for his dedication to my work and my committee members, Dr. Chen, Dr. Fayed, Dr. Chaudhary and Dr. Meeker, for their guidance and support throughout the course of this research.

Secondly, I would like to thank my friends, colleagues, and the department faculty and staff for making my time at Iowa State University a wonderful experience. Special thanks to Chen Zhao, Tao Zeng, Jingbo Duan, Srijita Patra and Chin-Wen Chen for both technical and personal support during my graduate study. I want to also offer my appreciation to those who were willing to participate in my studies and observations, without whom, this thesis would not have been possible.

In addition, I would also like to thank my bosses in TSMC, Eric Soenen and Alan Roth, who offered great opportunity for the internship and full-time job and provide great detail-orient technical support during my work. I appreciate their fully support and understanding while my last few month finishing this dissertation.

Finally, thanks to my family for their encouragement and dedication, and my boyfriend Chi-Chen Fang for his hours of patience, respect, and love.

SUPPORT ACKNOWLEDGMENTS

I was supported, in part, by the National Science Foundation (NSF), the Semiconductor Research Corporation(SRC), Texas Instruments, TxACE (through SRC), and the Tunc and Lale Doluca professorship.

ABSTRACT

Accurate, small and low-power CMOS temperature sensors designed for multi-position temperature monitoring of power management in multi-core processors are proposed. The temperature sensors utilize the temperature characteristics of the threshold voltage of a MOS transistor to sense temperature and are highly linear from 60°C to 90°C. This is the temperature range needed for the power management applications where temperature sensors are strategically placed at multiple locations in each core to protect the processor from temperature-induced reliability degradation. A temperature-to-digital converter (TDC) that does not require either a reference generator or an ADC is also introduced, and it exhibits low supply sensitivity, small die area, and low power consumption. Both analog threshold voltage based temperature sensor and a prototype TDC designed to support multi-position thermal-sensing for power management applications from 60°C to 90°C are implemented in an IBM 0.13μm CMOS process with a 1.2V power supply.

A new verification approach with several variants for identifying the number of stable equilibrium points in supply-insensitive bias generators, references, and temperature sensors based upon self-stabilized feedback loops is introduced. This provides a simple and practical method for determining if these circuits require a "start-up" circuit and, if needed, for verifying that the startup circuit is effective at eliminating undesired stable equilibrium points in the presence of process and temperature variations. These undesired stable equilibrium points are often referred to as Trojan states. It will be shown that some widely used approaches for verification do not guarantee Trojan states have been removed. Some of the methods introduced appear to be more practical to work with than others. A group of

benchmark circuit with Trojan states will be introduced and used to demonstrate the effectiveness of the new method.

CHAPTER 1

INTRODUCTION

An explosion in the demand for computer, tablet and mobile electronic devices has driven semiconductor manufacturers to aggressively scale down CMOS device dimensions. As a generalization of Moore's law, the downward scaling of feature sizes in semiconductor processes has been paralleled with a doubling of the number of components in an integrated circuit about every two years. Demand for high performance, intensive computation, and multi-functional processors has led to higher integration density, increased power density, larger thermal gradients, highly localized hotspots, and higher operating temperatures in the processors. Thermal management in modern processors has become a prominent and aggravating issue in computer systems design and managing or reducing total chip power is no longer sufficient for achieving target reliability metrics unless methods are also used for mitigating localized hotspots. Nowadays, multicore processors on a single chip dominate the industry but paralleling the evolution of the multicore architectures are a rapidly growing need for improved methods of dynamic power and thermal management. In order to achieve high efficiency and long-term reliability for multicore processors, accurate temperature sensors with low-power consumption and small-chip area are needed to provide sensory input to the power/thermal management units. A major component of this research initiative has been devoted to the design of practical temperature sensors suitable for use in on-chip power/thermal management blocks.

Since accurate temperature measurement has become recognized as a critical part of the power and thermal management of an integrated circuit that is needed to prevent

performance and reliability degradation, most researcher have focused on pursuing better performance by incorporating elaborate circuit design techniques such as digitally-assisted feedback loops to enhance performance of low dropout regulators, slew-rate enhancement to improve the high-frequency performance of amplifiers, and nested-compensation to improve the gain of the amplifiers when operating at low supply voltages. These elaborate techniques need to be carefully designed to avoid undesired artifacts such as inadequate phase margin, instability, etc. These elaborate techniques often use nonlinear components and involve the intentional or accidental creation of one or more positive feedback loops. Nonlinear circuits with one or more positive feedback loops are vulnerable to the presence of multiple operating points. Invariably the circuits are designed to operate at a single stable operating point and if multiple stable operating points are present, all operating points except the target operating point are undesired operating points. Unfortunately, the feedback and nonlinearities in these circuits often make it difficult or impossible to analytically determine the location of undesired operating points if they exist. And it is often even impossible to analytically determine the presence or absence of undesired operating points even if the location of the undesired operating point of not of concern. Although circuit simulators such as SPICE and SPECTRE are often used to find solutions of nonlinear circuits where analytical solutions are not possible, the presence or absence of undesired operating points in nonlinear circuits can often not even be determined with existing circuit simulators since circuit simulators will provide only one static solution of a nonlinear circuit for fixed points in the PVT domain. If designers recognize the presence of an undesired stable equilibrium point, special circuits are often added to eliminate the undesired stable equilibrium points. These circuits are often termed “startup circuits”. Even if a startup is included and even if the circuit initially starts

up, there is often not a guarantee that the circuit will always operate at the desired operating point. If the startup circuit is not robust, the circuit may jump to an undesired operating point due to temperature perturbations, noise transients, or perturbations on the supply bus. Thus, a systematic method is required to not only determine the vulnerability of a circuit to undesired equilibrium points but also to verify robustness of startup circuits when the need for a startup circuit has been identified. A second major component of this research initiative has been devoted to identifying the presence of positive feedback loops, on detecting the need of startup circuits, and on verifying the effectiveness of the startup circuits when they are required. This is a key component of the emerging field of verification of analog circuits.

1.1. Temperature Sensor and Temperature-to-Digital Converter

In modem VLSI design, on-chip thermal monitoring is becoming increasingly important for advancing technology. Multicore processors now offer better performance and efficiency than the single-core processors. However, large temperature gradients due to power variations from core to core result in “Hot Spots” on chip. The gradients and hot spots are of major concern and if unabated, will degrade the reliability and lifetime of the chip. Several different power/thermal management strategies have been used to mitigate thermal issues including throttling of the clock frequency, reassigning tasks among cores, reducing supply voltages, or automatic shutdown. These solutions usually require a large number of temperature sensors that are strategically distributed on the chip; therefore, very small easy-readout on-chip thermometers are needed. Throttling often is based upon a single predetermined temperature trigger [1]-[3] which, for safe operation, is usually set somewhere between 60 °C and 90 °C. More sophisticated throttling algorithms may be based upon a Boolean representation of the temperature in this same range.

In order to accomplish multi-core thermal control, the requirements of the on-die temperature sensor are quite strict. The sensors need to be very small so that they can be placed close to a small group of critical transistors. The temperature sensors should be power efficient to avoid extra errors from self-heating. And, the sensors need to be accurate enough to achieve target reliability goals with power/thermal management algorithms without severely degrading system performance. Simple but widely used power/thermal management algorithms use throttling of the operation of the circuit to keep the maximum temperature at any location on the die below a predetermined threshold that is established to guarantee the target MTF is achieved. It can be readily shown that a ±1.4◦C temperature measurement error at 73.6◦C will cause ±10% deviation of the target MTF for wear induced by electromigration if the circuit is operating continuously at the trigger temperature as shown in Fig. 1-1. A plot of the cumulative distribution function (CDF) of the failure time for electro-migration-induced failure using a log-normal distribution with shape parameters of $\sigma = 0.1$ and $\mu=20$ is shown in this figure. The total temperature error is the sum of the error in measuring the actual die temperature at trim plus the error in the temperature sensor itself. A typical uncertainty of the trim temperature in a production testing environment is ±0.5°C. If the trim temperature error is ±0.5°C, the accuracy required for the temperature sensor itself is ±0.9°C. Thus, for this work, the target accuracy of the on-chip temperature sensors for power /thermal management has been set at ±0.9°C throughout the (60°C, 90°C) temperature range.

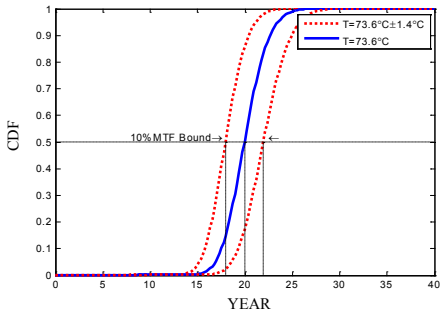


Fig. 1-1 CDF functions electromigration-induced failure with both thermal and electrical stress

Traditionally, the temperature dependence of the pn- junction has been used to sense temperature[4][5]. However, area and power consumed by on-chip pn-junction-based temperature sensors are not attractive and good accuracy is becoming increasingly difficult to obtain with the "parasitic" pn-junctions and the associated vertical "parasitic" bipolar transistors available in emerging semiconductor processes. Several papers have present high accuracy ($<\pm 0.2^{\circ}C$) pn-junction based temperature sensors [4]-[7]; however, good BJTs are either not available in modern CMOS processes or are based on parasitic BJTs which are not accurate, so various techniques are utilized to improve accuracy. Temperature sensors based upon the pn junction often require a low-offset operational amplifier. Dynamic offset cancellation such as chopping or auto-zeroing are often used to minimize the effects of input offset of the operational amplifier and dynamic element matching methods have been used to improve biasing matching characteristics. High accuracy sensors can be achieved by sacrificing area and power consumption. The average size of some of the reported ornate thermal sensors is around $0.1mm^2$ or larger which is not suitable for multi-position sensing for power management applications.

A time-to-digital temperature sensor [8][9] was published which is compatible with current CMOS technology. In this sensor, threshold voltage and transistor mobility jointly serve as the temperature sensing elements. In this sensor, the temperature dependence of the mobility induces an inherent nonlinearity with respect to temperature. An unattractive two-point calibration is necessary to achieve reasonable performance with this temperature sensor. Due primarily to the nonlinearity induced by the temperature-dependent mobility, curvature correction is also needed if higher accuracy required. The size of these sensors can be large as $0.6mm^2$ within $\pm 0.5^{\circ}C$ accuracy which is also not attractive for on-chip hotspot sensing.

The CMOS temperature sensors in [10]-[14] are based on the temperature dependence of mobility and/or threshold voltage or on the temperature dependence of thermal resistors. These sensors may require less area and lower power consumption. The authors of the papers presenting these temperature sensors claim they have acceptable temperature errors. Except for the sensor discussed in [10], all of these temperature sensors provide an analog output voltage or current that carries the temperature information. An analog-to-digital converter (ADC) is subsequently required to convert the voltage or current information into a Boolean representation of temperature. The temperature information in the sensor of [10] is carried in a frequency and a counter can be used to generate a Boolean output.

Almost all temperature sensors that provide a Boolean representation of temperature use the standard structure shown in Fig. 1-2. In addition to the temperature sensor, this structure has three ancillary blocks; an ADC, a reference generator, and a signal conditioner. For different applications, X_{SIG} can be a voltage, a time, a period, or possibly a current and

correspondingly the ADC can operate on voltages, currents, or maybe a time or period to digital converter. However, this standard approach has several limitations. First is the need of an ADC. Invariably the ADC consumes significant power and area. Second, the ADC needs a reference signal and good supply-insensitive reference generators, such as the standard Bandgap structures, also consume significant power and area. The area and power required for the signal conditioner can also be substantial. Finally, the performance of this structure is degraded by both the temperature and voltage dependence of the ancillary components.

The reported area requirements for the ADCs in [4]-[6]range in size between 0.1mm^2 and 4.5mm^2. In these designs, one-half or one-third of the total area is allocated to the ADC.

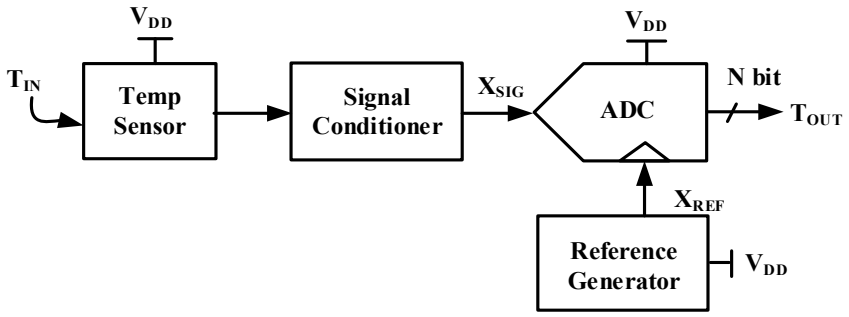


Fig. 1-2 Standard temperature to digital converter

In this work, a new approach to the design of temperature to digital converters (TDC) is introduced. With this approach, the reference generator, the ADC, and the signal conditioner shown in Fig. 1-2 are eliminated. A single comparator and some configuration switches internal to the temperature is all that is needed to build the TDC. With this approach, substantial reductions in area, power dissipation and supply sensitivity can be achieved while still obtaining good performance. In the circuits introduced in this work, the temperature dependence of the threshold voltage is used to sense temperature.

1.2. Verification of the Analog Circuits

Bias generators, references, and temperature sensors (BRT) are often built with a self-stabilizing feedback loop that inherently provides a low sensitivity of the output to variations in the supply voltage. Although a rigorous analytical characterization of the self-stabilizing feedback loop is seldom discussed in the circuit design community, most designers recognize that these circuits often require a "start-up" circuit to force these circuits to operate in the desired state and these start-up circuits are invariable included as part of the design.

The use of the term "start-up" circuit as a method for overcoming an inherent limitation in these self-stabilized loops is not particularly descriptive of the problem the "start-up" circuits are solving. Specifically, many of the more popular self-stabilizing feedback loops that are used for BRT applications have more than one stable operating point and the start-up circuits are used to eliminate the undesired stable operating points from the circuit.

Some results on the design of ultra-small, high-accuracy on-chip threshold-based temperature sensors for power/thermal management in multi-core systems based upon a supply-insensitive self-stabilizing feedback loop have been recently reported [13],[15] along with methods for guaranteeing that these circuits have a single stable equilibrium point. Others have focused specifically on the design better start-up circuits [16]-[19].

A standard practice in industry for verifying that a start-up circuit is effective is to run repeated transient simulations to verify that the BRT circuit "starts up" correctly, that is, to verify that the circuit operates as desired with an acceptable delay from the time the transient analysis starts. Although this approach often results in start-up circuits that serve the intended

purpose, it does not guarantee that all undesired stable equilibrium points have been eliminated. And, if all undesired stable equilibrium points have not been eliminated, an unanticipated sequence of transient events during normal operation can cause the circuit to move to an undesired stable equilibrium point. And even if the undesired stable equilibrium points have been eliminated for the conditions specified in the transient simulation, process and temperature variations may cause an undesired stable equilibrium point to reappear.

In this work, methods of verification of analog circuits are discussed that can be used to determine the presence or absence of undesired stable equilibrium points. These methods can also be used to determine whether a startup circuit is robust to PVT variations. The verification approach will be based upon a circuit-simulator based homotopy analysis whereby all positive feedback loops are identified. The homotopy analysis requires the simultaneously breaking all positive feedback loops so that the resultant "open-loop" circuit is guaranteed to have only one solution for any input thereby circumventing the open problem of finding all solutions to a set of nonlinear equations.

1.3. Organization

Two temperature sensors with analog outputs that can express threshold voltage are presented in Chapter 2. Circuit characteristics, design considerations, and reliability issue are discussed. Startup issues for these circuits are also discussed and a systematic method for verifying that these startup circuits remove undesired equilibrium points based upon a circuit-level homotopy analysis is introduced. This verification approach is extended in the discussion of analog circuit verification introduced in Chapter 4. Test chips of two temperature sensors were fabricated in TSMC 180nm and IBM 130 nm process. Experimental results verify the performance of these temperature sensors. A direct

temperature to digital converter that does not require an additional power and area hungry ADC or reference circuit is presented in Chapter 3. Analog verification methods focused on determining the presence or absence of undesired operating points are discussed in Chapter 4. A brief conclusion is presented in Chapter 5.

CHAPTER 2 TEMPERATURE SENSOR WITH ANALOG OUTPUT

2.1. Temperature Sensor with Linear Dependency to Temperature

Voltage references, bias generators, current references, current sources, and temperature sensors are all key building blocks that find widespread applications throughout the semiconductor industry. Although the intended use of these building blocks appears to be diverse, the circuit structures that are used to build these functional blocks are very similar and often identical. More specifically, it is often the case that a specific circuit used in one application serves as a bias generator, in another application it serves as a voltage reference, in another application as a current source, and in yet another application as a temperature sensor. One example of such a circuit is shown in Fig. 2-1. One way to view this circuit is to observe that transistors M_1 and M_2 and resistor R_5 form a Widlar Current Mirror and transistors M_3 and M_4 form a basic current mirror. These cross-coupled current mirrors generate a supply insensitive bias current which, in turn, generates supply insensitive output voltages V_{OUT1} and V_{OUT3}. Voltages V_{OUT1} and V_{OUT1} can be used as biasing voltages and when so used, it becomes a bias voltage generator. The circuit can also be designed so that the voltages V_{OUT1} and V_{OUT3} vary in a reasonably way with temperature. Thus, this circuit can serve as a temperature sensor as well. One interesting property of this and other generator circuits is that there is no "input" to the circuit beyond the supply voltage V_{DD} and the outputs of interest in the generator circuit are quite independent of V_{DD}. One key requirement of all practical generator circuits is that the outputs be quite independent of V_{DD} since the supply voltage is usually not accurately controlled and since considerable noise is usually present on the supply voltage bus due to switching transients inherently introduced by the circuit it is biasing.

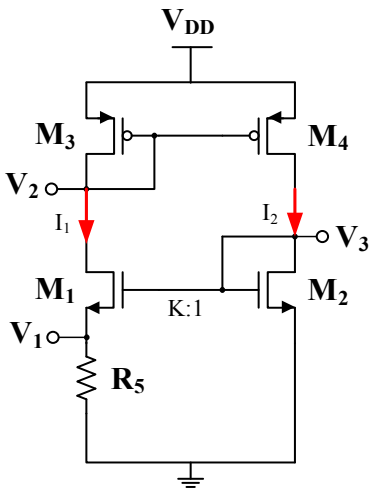


Fig. 2-1 Vdd-independent Widlar Bias Generator

2.1.1. Temperature sensor with positive temperature oefficient

As mentioned above, the bias generator shown in Fig. 2-1 can be designed to serve as a temperature sensor. The Widlar bias generator is also called a Beta-multiplier reference (BMR) [20]. The currents are determined by the design parameters; R_5, the ratio K of the sizes of M_1 and M_2, and the gain of the current mirror M_3:M_4. If the M_3:M_4 current mirror gain is 1 and the size ratio between M_1 and M_2 is K, and if the channel length modulation effect is neglected, the currents can be expressed as

$$I_1 = I_2 = I_{PTC} = \frac{2}{R_5^{\,2}\mu_n C_{OX}\frac{W_2}{L_2}} \cdot \left(1-\frac{1}{\sqrt{K}}\right)^2 \tag{1.1}$$

where I_1 and I_2 are the drain current of M_1 and M_2.

The temperature dependence of the currents I_1 and I_2 will now be characterized. The temperature dependence of the resistor R_5 will be assumed to be linear. Thus it can be expressed as a first-order temperature dependent model by the equation

$$R = R_0\left[1+\alpha(T-T_{NOM})\right] \tag{1.2}$$

where α is a process and material dependent parameter that is assumed to be independent of temperature. In this model, T is the temperature in K and T_{NOM} is any nominal temperature. For convenience, T_{NOM} is often 300K though it will be kept as a variable in this formulation. It will be assumed that the resistor has a positive temperature coefficient, that is, $\alpha > 0$. The temperature dependence of the mobility μ_n is modeled by the equation

$$\mu_n = \mu_0 \left(\frac{T}{T_{NOM}} \right)^{UTE} \tag{1.3}$$

where UTE is the mobility temperature exponent [22], typically between -2 and -1, and μ_0 is the mobility at T_{NOM} . Often μ_0 is specified at 300K. The first-order temperature dependence of the current can be obtained by taking the derivative of the reference current with respect to temperature to obtain the expression

$$\begin{aligned} \frac{dI_{PTC}}{dT} &= \frac{d}{dT} \cdot \left[\frac{2\left(1-\frac{1}{\sqrt{K}}\right)^2}{\left\{R_0\left[1+\alpha(T-T_{NOM})\right]\right\}^2 \mu_0 \left(\frac{T}{T_{NOM}}\right)^{UTE} C_{OX} \frac{W_2}{L_2}} \right] \\ &= \frac{2\left(1-\frac{1}{\sqrt{K}}\right)^2}{R_0^{\,2} \mu_0 C_{OX} \frac{W_2}{L_2}} \cdot \left[\frac{-2\alpha \left(\frac{T}{T_{NOM}}\right)^{-UTE}}{\left[1+\alpha(T-T_{NOM})\right]^3} + \frac{-UTE\left(\frac{T}{T_{NOM}}\right)^{-UTE-1}}{\left[1+\alpha(T-T_{NOM})\right]^2} \right] \end{aligned} . \tag{1.4}$$

Both the resistor and mobility are affected by temperature, but the temperature coefficient of the resistor is often sufficiently small so that the temperature coefficient of the mobility dominates the temperature dependence of the current. Since UTE is negative, it follows that the current has a positive temperature coefficient (PTC) when the temperature characteristics of the resistor are negligible. If the current flows through a resistor and the temperature

coefficient of the resistor are negligible, the temperature coefficient of the voltage across the resistor is also positive.

As can be seen from (2.1), the structure is immune to power supply variations when all transistor operate in the saturation region since it is self-stabilized. And it follows from (2.4) that if UTE is close to -1, a very linear voltage to temperature relationship can be achieved by adding R_B shown in Fig. 2-2 and taking the output, designated as V_{PTC}, across the resistor. A PTC voltage is generated as given in (1.5), and the temperature sensitivity is scalable with resistor.

$$V_{PTC} = I_{PTC} \times R_B \tag{1.5}$$

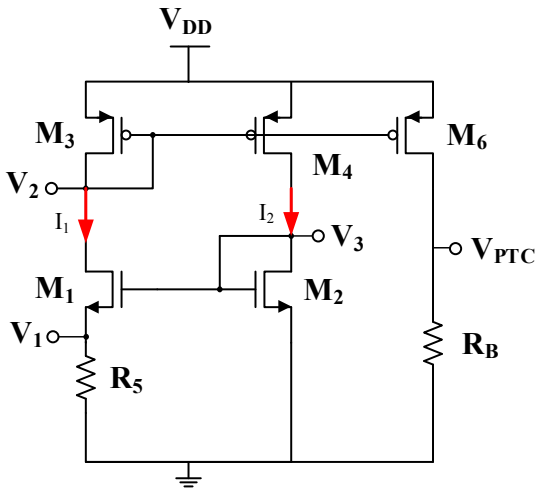


Fig. 2-2 Schematic of the proposed PTC temperature sensor

Since it is a self-bias positive feedback loop structure, stability should be verified at the desired operating point. The loop gain should be always less than one at the desired operating point to keep the circuit stable. By breaking the loop at either the gate node of M_4 or M_1, the circuit can be viewed as two cascaded common source amplifiers with one of them having the source degeneration resistor R_5. Assuming that all transistors are operating in the

saturation region at the desired operating point and neglecting the small-signal output conductrances, the small-signal loop gain, A_L , given in (1.5) can be readily obtained.

$$A_L = \frac{gm_1 gm_4}{gm_2 gm_3 (1 + gm_1 R_5)} \tag{1.6}$$

where $gm_k = 2I_{Dk} / V_{EBk}$ and $V_{EBk} = V_{gsQk} - V_{Tk}$ for $k \in \{1,2,3,4\}$ and where V_{Tk} is the threshold voltage of transistor k. Since the nominal value of the currents I_1 and I_2 are the same, the loop gain expression can be simplified to

$$A_L = \frac{V_{EB2}}{V_{EB1} + 2I_D R_3} \tag{1.7}$$

Where $I_D = I_1 = I_2$

Assuming the threshold voltages of M_1 and M_2 are the same and expressed as $V_{T1} = V_{T2} = V_T$, the excess biases V_{EB1} and V_{EB2} at the Q-point can be expressed as

$$\begin{aligned} V_{EB1} &= V_{gs1} - V_T \\ V_{EB2} &= V_{gs1} + I_D R_3 - V_T \end{aligned} . \tag{1.8}$$

By replacing V_{EB1} and V_{EB2} in (1.7) with (1.8), the loop gain become

$$A_L = \frac{V_{gs1} - V_T + I_D R_3}{V_{gs1} - V_T + 2I_D R_3} . \tag{1.9}$$

It follows from (2.9) that the loop gain is always less than one provided all devices are operating in the saturation region.

Though not apparent from the analysis presented in this section, a startup circuit is needed for this temperature sensor to eliminate an undesired stable equilibrium mode that is present at most temperatures and for most implementations of this circuit.

2.1.2. Temperature sensor with negative temperature coefficient

An output voltage with a negative temperature coefficient (NTC) can be obtained from the five-transistor inverse-Widlar (5TIW) bias generator shown in Fig. 2-3. As will be shown, the output voltages V_{1A} and V_{3A} are ideally proportional to the threshold voltage which is nominally linear with temperature and independent of the mobility which has anonlinear temperature dependence. Thus, this circuit serves as a linear temperature sensor. This circuit is a subcircuit in the temperature sensors discussed by Szekely [14], but rather than focusing on the output voltages this subcircuit provides, the authors in [14] reported on the output current which is a function of both the threshold voltage and mobility. Thus the temperature sensor of Szekely does not have a linear relationship with temperature. An analytical expression for the output of the 5TIW will now be derived.

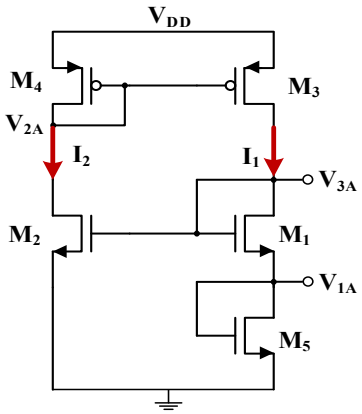


Fig. 2-3 Schematic of five-transistor inverse-Widlar (5TIW) bias generator

If a square-law model for the transistors in the 5TIW is used and if output conductance effects, channel length modulation, and body effects are neglected, it follows from a standard circuit analysis that the circuit is characterized by the group of equations in (1.10).

$$\begin{cases} \frac{1}{2}\mu_n C_{ox}\left(\frac{W}{L}\right)_1 \left(V_{3A}-V_{1A}-V_{T1}\right)^2 = I_1 \\ \frac{1}{2}\mu_n C_{ox}\left(\frac{W}{L}\right)_5 \left(V_{1A}-V_{T5}\right)^2 = I_1 \\ \frac{1}{2}\mu_p C_{ox}\left(\frac{W}{L}\right)_3 \left(V_{DD}-V_{2A}-V_{T3}\right)^2 = I_1 \\ \frac{1}{2}\mu_n C_{ox}\left(\frac{W}{L}\right)_2 \left(V_{3A}-V_{T2}\right)^2 = I_2 \\ \frac{1}{2}\mu_p C_{ox}\left(\frac{W}{L}\right)_4 \left(V_{DD}-V_{2A}-V_{T4}\right)^2 = I_2 \end{cases} \tag{1.10}$$

Assuming that M_3:M_4 current mirror has a gain equal to 1, and assuming the size of M_3 and M_4 and their threshold voltages are the same, the analytical expression of the outputs V_{1A} can be obtained by solving the equations in (1.10). The solution is shown in (1.11).

$$V_{1A} = \frac{\eta_{15}\left(V_{TH2}-V_{T1}\right)+\left(1-\eta_{12}\right)V_{T5}}{1+\eta_{15}-\eta_{12}} \tag{1.11}$$

where $\eta_{mn} = \sqrt{\frac{(W/L)_m}{(W/L)_n}}$. The output V_{1A} is a linear function of the threshold voltages of N-channel devices and transistor size ratios. It is important to observe specifically that it is supply independent and independent of all other model parameters. Thus, with the models used for the transistors, the temperature dependence of V_{1A} is completely determined by the temperature dependence of the threshold voltages V_{T1}, V_{T2}, and V_{T5}.

According to the threshold voltage temperature dependence model in [22], the threshold voltage itself is nearly linear with respect to temperature and can be expressed as:

$$V_{tn}(T) = V_{tn0} + (KT1 + KT1L \times \frac{L}{L_{eff}} + KT2 \times V_{bseff}) \times \left(\frac{T}{T_{NOM}} - 1 \right) \tag{1.12}$$

In the V_T temperature model, V_{tn0}, KT1, KT1L and KT2 are all constant process parameters and T_{NOM} is an arbitrary nominal temperature. The parameters KT1, KT1L and KT2 are dependent upon T_{NOM}. Often the model parameter's are defined for T_{NOM}=300K. The parameters KT1, KT1L and KT2 jointly determine the first-order temperature coefficient of V_{1A}. The effects of the parameter KT1L on the first-order temperature coefficient is scaled by the transistor length but will not affect the temperature linearity. The effects of KT2 on the threshold voltage is scaled by the effective voltage across the bulk and source terminals so V_{bseff} variations with temperature or V_{DD} changes with temperature will degrade output voltage linearity. In an n-well bulk CMOS process, the bulk-source voltage of M_2 and M_5 are both zero so KT2 for these transistors will not contribute to nonlinearity however the bulk of M_1 is separated from the source and this will introduce nonlinearity in the output voltage temperature dependence. But the nonlinear temperature dependence should be small. Since the voltage V_{1A} is nearly linear with respect to temperature, this circuit serves as a temperature sensor. This circuit will be denoted as the 5T VTH-based temperature sensor throughout the remainder of this thesis.

It can also be shown from (2.10) that V_{3A} is also a function of only the threshold voltages and device dimensions. Thus, both V_{1A} and V_{3A} can be used as the output of a temperature sensor. The voltage V_{3A} has a larger absolute value and a larger temperature coefficient which may be more attractive in many temperature sensor applications. However,

unless stated to the contrary, it will be assumed for convenience that V_{1A} is the output of the 5T VTH-based temperature sensor to facilitate comparison with other structures that will be discussed in this thesis.

As was the case for the PTC circuit in the previous section, the 5T VTH-based temperature sensor is also self-biased and contains a positive feedback loop so the issue of stability must be addressed. In particular, the loop gain of the positive feedback loop must be less than 1 at the desired operating point. For the 5T circuit, if the positive feedback loop is broken at the gate of M_2, the loop gain can be calculated by inserting a small-signal voltage source at the gate of M_2 and looking at the gain from this input to the output on the drain of M_1. The corresponding open-loop circuit is shown in Fig. 2-4. If the small-signal output conductances are neglected, it can be shown from a standard small-signal analysis that the loop gain is given by the equation in (1.13),

$$\text{Loop Gain} = \frac{gm_2 gm_3 (gm_1 + gm_5)}{gm_1 gm_4 gm_5} \tag{1.13}$$

Where the *gm* parameters are the small-signal transconductances of the corresponding transistors. Expressing each g_m in the form of $gm = 2I_D / V_{EB}$ where I_D is the quiescent drain current and V_{EB} is the excess bias voltage, and assuming the M_4:M_3 mirror gain is unity, the loop gain can be expressed as

$$\text{Loop Gain} = \frac{V_{EB3}}{V_{EB4}} \frac{V_{EB1} + V_{EB5}}{V_{EB2}} = \frac{V_{3A} - 2V_{TH}}{V_{3A} - V_{TH}} \tag{1.14}$$

It is apparent that the loop gain is less than 1 at the desired operating point so the desired operating point where (1.11) is satisfied is a stable equilibrium point.

Due to the positive feedback loop, this circuit is vulnerable to the presence of more than one stable operating point. This vulnerability is often viewed as the well-known startup issue. For many implementations, the circuit actually has two stable operating points over a wide temperature range with one of the stable operating points corresponding to a near-zero output voltage. The near-zero output voltage represents an undesired operating when this circuit is serving as a temperature sensor and a startup circuit is needed to remove the near-zero stable operating point. A discussion of the operation of this circuit follows.

The circuit can be viewed as the cascade of two common source inverting amplifiers connected in a positive feedback loop. If the loop is broken at the gate of M_2 by partitioning the node to which the gate of M_2 is connected into 2 nodes, as shown in Fig. 2-4, one of the new nodes is a high impedance node and the other is a low impedance node. If a voltage is applied at the resultant high-impedance node and the resultant low-impedance node is designated as the output node, the relationship between V_{OUT} and V_{IN} can be calculated. This relationship is termed the return map. Since the loop is broken at the gate to a MOS transistor, the break does not alter the loading in the "resistive network[1]" at the output node and all solutions of the original circuit occur at the intersection of the return map with the $V_{OUT} = V_{IN}$ line. At each intersection point the small signal loop gain can be calculated. The

[1] In this context, "resistive network" refers to the circuit obtained by setting all energy storage elements to their zero value, i.e. replacing all capacitors with open circuits and all inductors with short circuits

small signal loop gain at an intersection point is the slope of the return map at that intersection point. The intersection points are often termed equilibrium points.

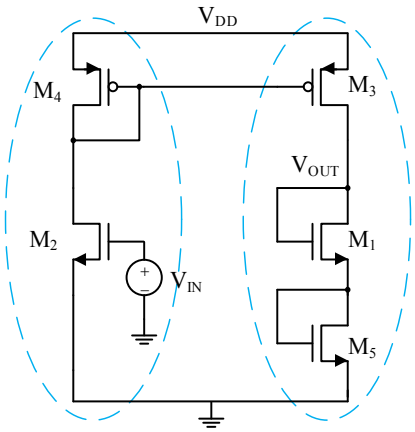


Fig. 2-4 Break-loop configuration of 5T temperature sensor

Equilibrium points for a circuit can be partitioned into two mutually exclusive groups. One group is comprised of those equilibrium points that are stable equilibrium points. An equilibrium point is a stable equilibrium point if the circuit will remain indefinitely at that operating point when initially forced to that point and will converge to that operating point as time goes to ∞ if forced to any point in a very small neighborhood from that point. An equilibrium point that is not a stable equilibrium point is an unstable equilibrium point. Whether equilibrium points in a resistive circuit correspond to stable or unstable equilibrium points in the corresponding circuit when energy storage elements are included can be determined from the return map of the resistive circuit. This binary classification of equilibrium points is summarized in the following conjecture. This has been listed as a conjecture rather than as a theorem because it will be presented without proof and because I do not have a reference for this theorem.

Equilibrium Point Classification Conjecture:

Consider the resistive circuit corresponding to a nonlinear stationary circuit that has one or more energy storage elements and a single positive feedback loop in the resistive circuit. If the small signal loop gain of the positive feedback loop is less than unity at an equilibrium point of the return map, then the equilibrium point is a stable equilibrium point and if the loop gain is larger than unity at an equilibrium point the equilibrium point is an unstable equilibrium point.

This conjecture does not provide a classification in the case where the loop gain at an equilibrium point is equal to unity. This condition has been intentionally excluded because it is believed to be of no practical significance.

Fig. 2-5 shows the return map for an implementation of the 5T Inverse-Widlar temperature sensor designed in a TSMC 0.18um process and simulated at 125°C. Device sizes used in this simulation are given in Table 2-1. There are 3 intersection points of the return map with the V_{OUT}=V_{IN} line. The intersection point where the gain is larger than one is an unstable operating point of the original circuit. The other two intersection points are stable equilibrium points. The upper stable equilibrium point is the desired operating point and the lower stable equilibrium point is an undesired operating point. If the initial conditions at time t=0 for the original circuit are set to force operation at the unstable equilibrium point, the voltage V_{1A} will either diverge to the high or the low stable equilibrium point. To prevent operation at the low stable equilibrium point, a start-up circuit can be added. The start-up circuit should be designed to eliminate the undesired operating point without altering the performance when operating at the desired equilibrium point. The start-up circuit should not eliminate the positive feedback loop.

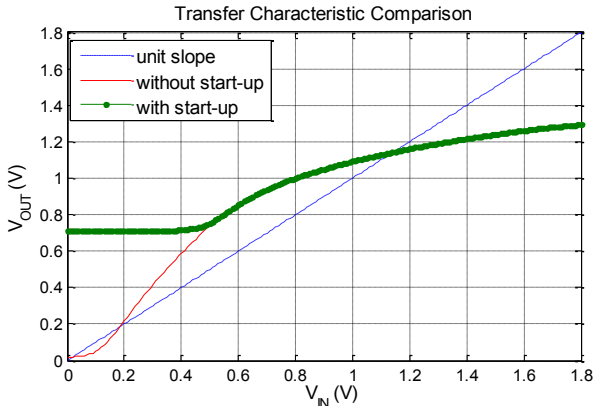


Fig. 2-5 Transfer characteristics of five-transistor Widlar-type temperature sensor

A simple start-up circuit comprised of the transistor M_s is shown in Fig. 2-6. With the start-up circuit included and the transistor sized as indicated in Table 2-1, a revised return map can be obtained. The return map as modified by transistor M_5 is also shown in Fig. 2-5. Note that in the vicinity of the desired operating point the return map is not modified by the start-up ciruit but the undesired operating point has been removed with completely removed with the start-up circuit. Thus, the return map method was not only useful for identifying the presence of the undesired operating point in the original, it was also useful for showing that the start-up circuit is effective in the revised circuit.

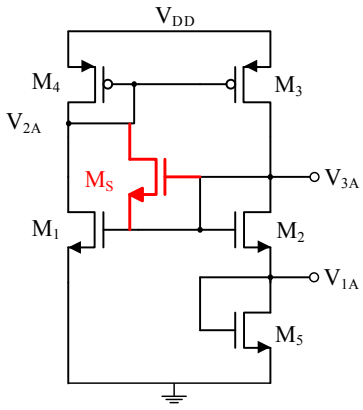


Fig. 2-6 Temperature sensor with start-up device

Table 2-1 Design size of 5T Widlar-type temperature sensor

Device	Size:(W/L)*M	Device	Size:(W/L)*M
M_1	5μm/0.4μm	M_4	4.5μm/0.9μm
M_2	0.3μm/0.6μm	M_5	7μm/0.4μm
M_3	4.5μm/0.9μm	M_s	0.5μm/1μm

The model of the transistor used in the derivation of (1.15) did not include the finite output conductance that is present in all transistors. If the finite output conductance had been included in the device models, a closed-form analytical expression for the output voltage would not have been obtained due to the additional complexity this modification would have added to solving a set of nonlinear equations. It can be shown that in addition to the increased analytical complexity, the finite output impedance also significantly degrades the linearity of the output with temperature. This degradation in linearity can be substantially reduced by using cascoding of the transistors to increase the effective output impedance of the devices but headroom often becomes a major limiting factor in determining whether cascading is a viable option for enhancing performance. In the following section, a four transistor bias generator with linearity performance similar to that achievable with the 5T temperature sensor will be discussed. The four transistor structure can offer one big advantage over the 5T temperature sensor and that is the option for full cascoding to dramatically reduce the effects of the finite output impedance of the transistors. A four transistor temperature sensor is discussed in the following section of this dissertation.

2.1.3. Dual-threshold voltage temperature sensor

A 4-transistor dual-threshold temperature sensor is shown in the Fig. 2-7. A process that has transistors with two distinct threshold voltages is required for implementing this circuit. In this circuit it is assumed that the threshold voltage of M_1 is larger than that of M_2.

This 4-transistor structure has enough headroom for full cascoding and can operate at very low supply voltages without having headroom problems. And a start-up circuit is often not required for implementations of the 4-transistor temperature sensor.

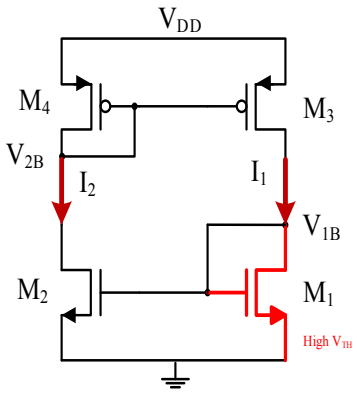


Fig. 2-7 Dual-Threshold four-Transistor(4Tt) temperature sensor

The output voltage for the 4-transistor temperature sensor in Fig. 2-7 will now be derived. Ignoring the output conductance effects and assuming the transistors are operating in strong inversion saturation and characterized by the ideal square-law model, it follows that:

$$\begin{cases} \frac{1}{2}\mu_n C_{ox}\left(\frac{W}{L}\right)_1 \left(V_{1B}-V_{T1}\right)^2 = I_1 \\ \frac{1}{2}\mu_p C_{ox}\left(\frac{W}{L}\right)_3 \left(V_{DD}-V_{2B}-V_{T3}\right)^2 = I_1 \\ \frac{1}{2}\mu_n C_{ox}\left(\frac{W}{L}\right)_2 \left(V_{1B}-V_{T2}\right)^2 = I_2 \\ \frac{1}{2}\mu_p C_{ox}\left(\frac{W}{L}\right)_4 \left(V_{DD}-V_2-V_{T4}\right)^2 = I_2 \end{cases} \tag{1.16}$$

If it is assumed that the M_4:M_3 mirror gain is 1, solving equations in (1.16) results in the output voltage expression

$$V_{1B} = \frac{\eta_{12} V_{T1} - V_{T2}}{\eta_{12} - 1} \tag{1.17}$$

where $\eta_{12} = \sqrt{(W/L)_1 / (W/L)_2}$. The output voltage given in (2.16) is the desired output voltage and this solution of the equations in (2.15) is unique. It should be observed, however, that even though this solution is unique, it cannot be concluded that the circuit has a unique solution. For example, if one or more of the transistors was operating in another region, such as weak inversion saturation, strong inversion triode, or some other region, the equations that characterize the circuit would differ from those of (2.15) and from the analysis just presented, it cannot be determined whether one or more additional solutions exist.

Under the assumption that all transistors are operating in strong inversion saturation, as was implicitly assumed to obtain the analytical expressions in (2.15), the voltage V_{1B} has to be larger than V_{T2}. As shown in (2.17), to achieve this relationship, it is necessary that V_{T1} must be larger than V_{T2}

$$\begin{aligned} &\frac{\eta_{12} V_{T1} - V_{T2}}{\eta_{12} - 1} > V_{T2} \\ &\therefore V_{T1} > V_{T2} \end{aligned} \tag{1.18}$$

It can be observed from (2.17) that the output of (2.16) is a function of the threshold voltage. This same observation was made for the output voltage V_{1A} of the 5T temperature sensor and thus it follows that the four transistor dual-threshold circuit also serves as a temperature sensor with an output that is quite linear with temperature.

In addition to the reduced headroom restrictions provided by the four transistor temperature sensor, the circuit provides the added advantage of eliminating the body effect when implemented in an n-well bulk CMOS process when compared to the 5T temperature

sensor of Fig. 2-3 since all NMOS transistors bulk nodes are connected to their sources which forces V_{bseff} in (2-12) equal to zero.

As was previously observed, the loop gain of a circuit with a single positive feedback loop must be less than unity at the desired operating point. It can be shown that the four-transistor dual-threshold temperature sensor has a single positive feedback loop. Following an analysis similar to that used for the 5T temperature sensor, the positive feedback loop can be broken at the gate of transistor M_2 to obtain the small-signal loop gain. For the four-transistor dual-threshold temperature sensor, if the output conductances of the transistors are neglected, the small-signal loop gain at the desired operating point can be expressed in terms of the small signal model parameters as given in (1.19).

$$. A_{VL} = \frac{gm_2 gm_3}{gm_1 gm_4} \tag{1.19}$$

The stability requirements will now be obtained under the assumptions that all transistors are operating in strong inversion saturation and the M_4:M_3 current mirror gain is unity. Since the mirror gain is unity, gm_3=gm_4. Thus, the requirement that the loop gain be less than unity results in the following sequence of equations:

$$\begin{gathered} gm_2 / gm_1 < 1 \\ \frac{2I_2}{V_{EB2}} \Big/ \frac{2I_1}{V_{EB1}} < 1 \\ V_{EB1} < V_{EB2} \\ V_{1B} - V_{TH1} < V_{1B} - V_{TH2} \\ V_{TH1} > V_{TH2} \end{gathered} \tag{1.20}$$

Since the high V_T device is always used for M_1, the circuit is stable. Alternatively, it can be stated that the loop gain will be less than 1 provided that V_{TH1}>V_{TH2}. From a practical perspective, for this circuit to be useful, the threshold voltage of M_1 must be larger than that

of M_2 over PVT variations. Throughout the remainder of this thesis, the dual-threshold four-transistor temperature sensor will be referred to as the 4T temperature sensor.

The issue of the uniqueness of the solution of the 4T temperature sensor will now be addressed. The open loop transfer characteristics of the 4T temperature sensor with the loop broken at the gate of M_2 are shown in Fig. 2-8 for various device sizes where V_{TH1} and V_{TH2} are the two n-channel threshold voltages with $V_{TH1}>V_{TH2}$. From these transfer characteristics, it can be seen that irrespective of the devices, the transfer characteristics have a unique intersection point with the unity loop gain line and thus the circuit has a unique solution. Thus, a start-up circuit is not needed to guarantee that this circuit has a single stable equilibrium point. It can also be observed from this figure that for the circuit to have all devices operating in the saturation region, a necessary condition for low V_{DD} sensitivity, the devices must be sized so that the loop gain is less than 1.

Simulation results for the non-cascode 4T transistor designed in a IBM 0.13µm CMOS process with n-channel threshold voltages of V_{Tn1}=450mV and V_{Tn2}=380mV and with device sizes given in Table 2-2 are shown in Fig. 2-9. These simulations were made at a temperature of T=27^{o}C,V_{DD}=1.2V for typical/typical process parameters, These simulation results show a single solution thus substantiating the earlier observation that a start-up circuit is not needed for the 4T temperature sensor at the simulation point in the PVT domain used in these simulations. Although these simulation results were obtained at a single point in the PVT domain, simulations also have been run at slow/slow process corner with 1.08V and fast/fast process corner with 1.32V and all simulations show only a single intersection point thus confirming that a start-up circuit is not needed for the 4T temperature sensor.

Table 2-2 Non-Cascode 4T Temperature Sensor

Device	Size:(W/L)*M	Device	Size:(W/L)*M
M_1	(3.8μm/2μm)*2	M_3	(3μm/1μm)*4
M_2	(0.3μm/1μm)*1	M_4	(3μm/1μm)*4

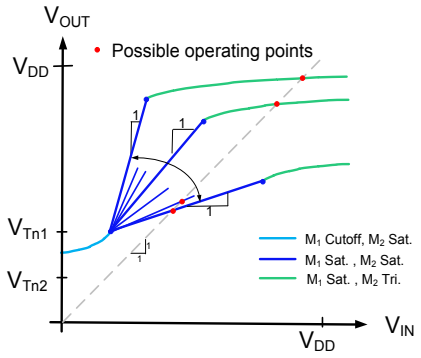


Fig. 2-8 Transfer characteristics of dual-threshold sensor with $V_{T1}>V_{T2}$

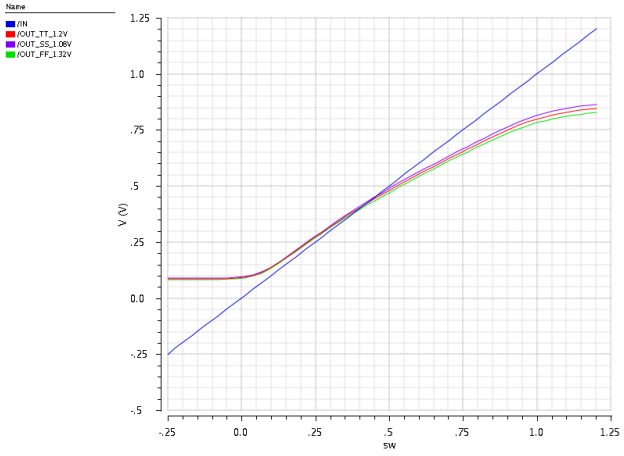


Fig. 2-9 Dual-threshold temperature sensor transfer characteristic

A fully-cascoded version of this temperature sensor is shown in Fig. 2-10. Transistor M_1 is the high V_T transistor. All other transistors are normal V_T transistors. The cascaded version has larger output impedance which gives much low sensitivity of power supply.

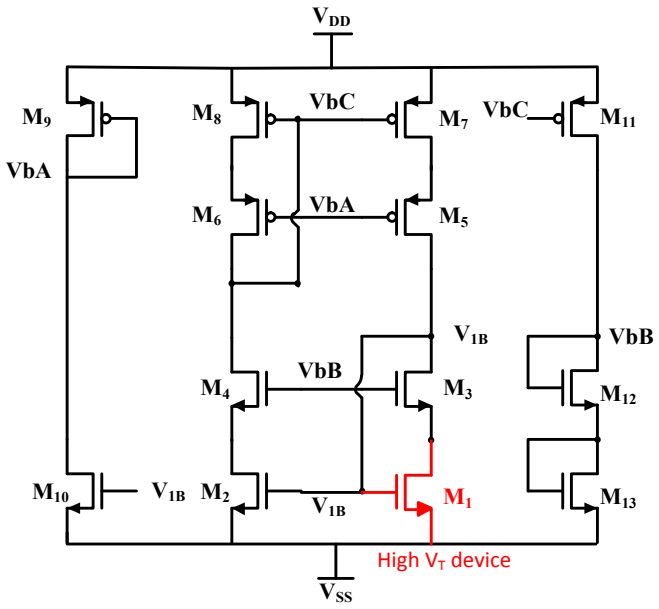


Fig. 2-10 Schematic of cascode 4T temperature sensor

2.1.4. Simulation results

The circuits are designed and simulated by Spectre. This section will show the non-cascode and cascade version of 5TIW and Dual-Threshold 4T temperature sensor respectively. All 5TIW circuits are designed in TSMC 0.18µm process with 1.8V supply, and 4T temperature sensors are designed in IBM 0.13µm process with 1.2V. The size of 5TIW non-cascode temperature sensor is shown in Table 2-1. Simulation results of V_{1A} and its INL are shown in Fig. 2-11. The thermal INL is defined to be the difference between V_{1A} over temperature and its end-point fitting-line. With the process variation, V_{1A} can drift +/- 35mV, yet V_{1A} still remains good linearity at different corner. Table 2-3 shows the corresponding value of Fig. 2-11. Temperature coefficient is the slope of V_{1A} in Fig. 2-11, and it shows this sensor can provide stable thermal sensing output.

The cascode version is shown in Fig. 2-12, the startup circuit and bias circuit is included. Table 2-4 shows the device size of the cascode 5TIW. The cascode version should gain the benefit from cascoding the current mirror; however, due to limitation of headroom, the performance actually degrade over process and supply vatiation. The simulation results are shown in Fig. 2-13. For the Typical-Typical process, the linearity is better compares to the non-cascode one, but the overall linearity over corners have some variation, yet still with acceptable linearity. For the low supply, devices are near triode resgion due to less headroom.

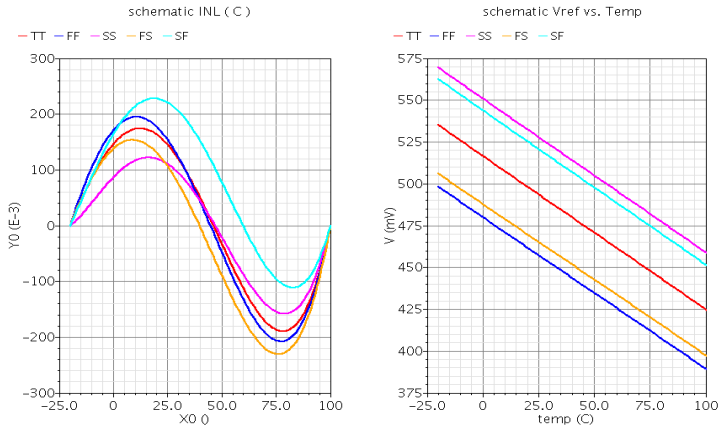


Fig. 2-11 Simulation results of 5T VTH-based temperature sensor over corner (a) Thermal INL (b) V1a

Table 2-3 Simulation data of 5T V_{TH}-based temperature sensor

Corner(Fig. 2-11)	Temperature Coefficient(10^{-3})	Error(INL) ^{o}C
TT	-0.92	0.185
FF	-0.91	0.21
FS	-0.92	0.145
SF	-0.91	0.22
SS	-0.93	0.241
Supply		
Vdd=1.98	-0.93	0.3
Vdd=1.62	-0.91	0.61

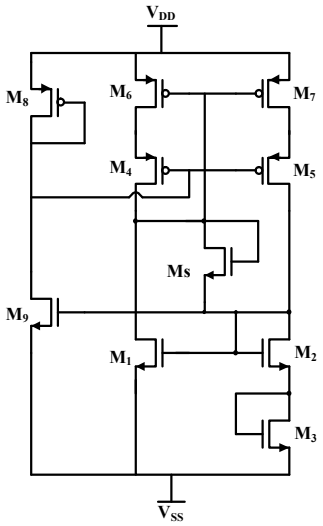


Fig. 2-12 Schematic of cascode 5T temperature sensor

Table 2-4 Device size of cascode 5T temperature sensor

Device	Size:(W/L)*M	Device	Size:(W/L)*M
M_1	5μm/0.4μm	M_6	7μm/0.4μm
M_2	0.3μm/0.6μm	M_7	7μm/0.4μm
M_3	4.5μm/0.9μm	M_8	0.5μm/1μm
M_4	4.5μm/0.9μm	M_9	7μm/0.4μm
M_5	7μm/0.4μm	Ms	0.5μm/1μm

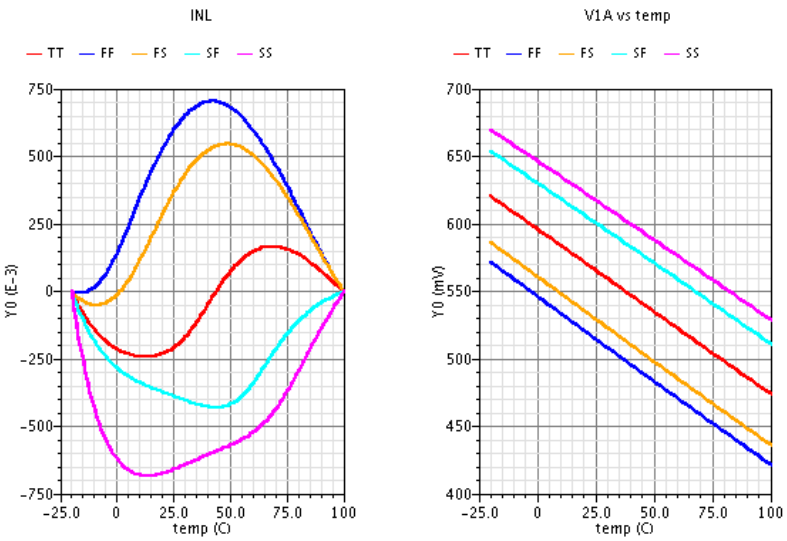


Fig. 2-13 Simulation results of Cascode 5T VTH-based temperature sensor over corner (a) Thermal INL (b) V1b

Table 2-5 Simulation data of cascode 5T VTH-based temperature sensor

Corner(Fig. 2-12)	Temperature Coefficient(10^{-3})	Error(INL) ^{o}C
TT	-1.17	0.16
FF	-1.219	0.7
FS	-1.25	0.54
SF	-1.249	0.43
SS	-1.187	0.68
Supply		
Vdd=1.98	-1.237	0.71
Vdd=1.62	-1.171	1.4

Dual-Threshold temperature sensors are designed in IBM 0.13um 1P6M process with 1.2V supply, both non-cascode and cascode version are simulated in five corners and ±10% supply to verify the performance over process and voltage variation. Table 2-6 listed the design size.

Table 2-6 Device size of cascode Dual-Threshold based temperature sensor in Fig. 2-10

Device	Size:(W/L)*M	Device	Size:(W/L)*M
M_1	(3.8u/2u)2	M_7	(3u/1u)8
M_2	(0.3u/1u)1	M_8	(3u/1u)8
M_3	(1.2u/0.32u)8	M_9	(3.4u/1u)
M_4	(1.2u/0.32u)8	M_{10}	(0.3u/1u)1
M_5	(3u/1u)4	M_{11}	(3u/1u)4
M_6	(3u/1u)4	M_{12}	(0.3u/1.8u)1

Fig. 2-7 and Table 2-2 in Sec.2.1.1 shows the schematic and dimension size of Non-Cascode Dual-Threshold temperature sensor, and Fig. 2-14 and Table 2-7 shows the simulation results related to the design. Since there is only one N-channel transistor on the left branch, the circuit has more headroom compares to 5TIW version. The simulation results have smaller impact due to supply variation especially with lower power supply.

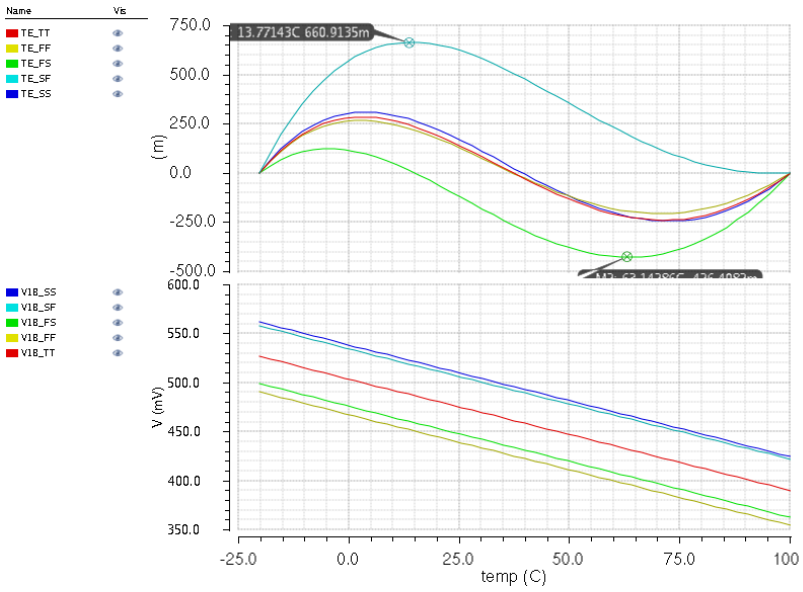


Fig. 2-14 Simulation results of the non-Cascode Dual-Threshold temperature sensor in Fig. 2-7

Table 2-7 Simulation data of Dual-Threshold temperature sensor

Corner(Fig. 2-13)	Temperature Coefficient(10^{-3})	Error(INL) ^{o}C
TT	-1.13	0.25
FF	-1.125	0.26
FS	-1.1328	0.45
SF	-1.129	0.66
SS	-1.1416	0.3
Supply		
Vdd=1.32	-1.111	0.478
Vdd=1.08	-1.15	0.505

2.2. Aging Characteristic of V_{TH} Based Temperature Sensor Circuit

Reliability of all integrated circuits is of concern. In many circuits, reliability is primarily associated with device failure that will render an integrated circuit non-functional.

In some precision analog integrated circuits, reliability is more associated with parametric drift with time which can cause the circuit to drift out of specs. Since temperature sensors are precision analog circuits and since some design approaches are highly sensitive to model parameters, the vulnerability of the performance of temperature sensors to wear-induced variation in model parameters must be addressed. There are a large number of papers published on the topic of precision temperature sensors [3-15] but few researchers have addressed the issue of reliability.

Meijer [23] discusses the long-term stability of parasitic bipolar transistors in CMOS technology that form the basic temperature sensing element in several variants of the pn-junction based proportional to absolute temperature (PTAT) temperature sensors. The authors claim that most inaccuracy problems in these temperature sensors can be solved by dynamic signal processing techniques. They further observed that the mechanical stress in a CMOS process is less than in the conventional Bipolar process which is a favorable property. They indicated that the long-term stability is attributable to drift which is caused by the mismatch of thermal coefficient induced thermal and time dependent mechanical stress. The package gives certain pressure to the component, fortunately, CMOS device using PNP substrate transistors which has about two to seven times less stress than the bipolar process.

In addition to the drift due to mechanical stress, there are several wear out mechanisms that degrade component lifetime, such as time-dependent gate oxide breakdown (TDDB), Channel Hot Carrier (CHC), negative bias temperature instability (NBTI), stress migration, leakage current, electromigration, and radiation induced soft errors .These mechanisms may change device parameters which can affect the performance of

many analog circuits and cause the circuit to operate out of specifications or, in extreme cases, can cause a circuit to fail.

Shor [10] discussed a CMOS V_{TH}-based temperature sensor which was used for multi-site temperature sensing in the Intel Sandy Bridge Processor [45] which went into production in the 32nm process node. Shor [3] subsequently claimed that "*over the course of the process lifetime, V_{TH} and μ can change, limiting reliability"*, and based upon this claim changed his focus to BJT-based temperature sensors where temperature is sensed through the temperature dependence of the pn junction. Implicit in his claim and subsequent change in approach is the premise that BJT-based temperature sensors are more reliable than V_{TH}-based structures. Shor did not, however, provide any insight, analytical formulation, or experimental results that compared the reliability performance of the V_{TH}-based structures with the BJT-based temperature sensors nor did he provide comments about what failure mechanisms he associated with the term "*limiting reliability*". Considering the fact that the V_{TH}-based temperature sensors reported by Shors [10] are simple circuits comprised of widely used analog blocks that comprise many different analog and mixed-signal circuits that are considered to be reliable by industry and considering the fact that the V_{TH}-based temperature sensors were used in the Sandy Bridge processor which was the flagship processor of Intel at the time it was released, it must be concluded that the reliability concerns were associated with potential drift in accuracy of the temperature and not with some form of catastrophic failure of the temperature sensor. Drifts in accuracy of any V_{TH}-based temperature sensor are strongly dependent upon the architecture used in the implementation as well as the device sizing and power levels used in the design making it difficult to make generalized statements about reliability of V_{TH}-based temperature sensors.

The Sandy Bridge processors did have a reliability problem and there was a massive recall of the Sandy Bridge processors by Intel due to stress-based failures that occurred on a small percentage of the production parts. But that recall was not associated with the reliability of the V_{TH}-based temperature sensors.

In what follows, threshold voltage degradation mechanisms associated with a drift in performance of MOS transistors will be discussed. This information should be useful for analytically and quantitatively predicting the reliability of V_{TH}-based temperature sensors attributable to aging-induced wear mechanisms in the transistors. Predictions of the time-dependent wear-induced threshold voltage shift will be based on the stress model discussed by Wang [24] and Maricau's [25].

Several CMOS temperature sensors including those in [9,10,14] as well as the 5T temperature sensor discussed in Section 2.1.2 are based, at least in part, on use of the threshold voltage of the MOSFET as a temperature sensing parameter. In some, including the 5T temperature sensor, the threshold voltage of the MOSFET is the dominant temperature sensing parameter. Channel Hot Carrier (CHC) and negative bias temperature instability (NBTI) are the two main contributors to the time-dependent shift in the threshold voltage. These two phenomenal are discussed in the following section.

2.2.1. Channel hot carrier (CHC)

Short channel devices, especially when the length of the MOS transistors is less than 0.35μm, may suffer from high electrical field-induced carrier heating if the drain-source voltage is large. The transistors experience high lateral electrical field in the pinch-off region and hence heat up the carrier. When the carriers get enough energy from the high lateral

electrical field, those hot carriers scatter and inject into the gate oxide. This injection causes hole trapping, electron trapping or interface state generation depending on different bias conditions. This damage to the gate oxide modifies device model parameters such as the threshold voltage which, in turn, will modify drain current and transconductance when the devices are embedded in a circuit. Normally, the generation of interface states dominants the damage of NMOS devices when V_{GS} is biased between V_{TH} and V_{DS} and worst-case damage occurs when the substrate current is at its maximum value [26]. It was shown in [26] that the substrate current increases with V_{DS} and for a given V_{DS}, the maximum occurs when $V_{GS} \approx 0.5V_{DS}$ so this corresponds to the worst bias condition. For p-channel devices, CHC causes less degradation than for n-channel devices since the majority carriers have less energy and thus fewer hot carriers will be generated.

Wang [24] creates an analytical CHC model based on the reaction – diffusion (R-D) approach for hot carrier degradation to simulate the threshold voltage shift.

$$\Delta V_{TH} = \frac{q}{C_{OX}} K_2 \sqrt{Q_i} \exp\left(\frac{E_{OX}}{E_{O2}}\right) \exp\left(-\frac{\varphi_{it}}{q\lambda E_m}\right) t^{n'} \qquad (1.21)$$

where K_2, E_{02}, and n' are process parameters that are determined for each process node from measurement results. Q_i is the inversion charge that is dependent on the transistor excess bias voltage, E_{OX} is the vertical electrical field, E_m is the lateral electrical field, λ is the mean free path, and ϕ_{it} is the minimum impact ionization energy in electronvolts. The models for Q_i, E_{OX}, and E_m as well as typical values for K_2, ϕ_{it}, n', and λ are given in Table 2-8 below. It can be observed that as the channel length shrinks, threshold voltage degradation due to CHC is worse since E_m increases as the effective channel length decreases. Compared to NBTI, recovery of CHC effect is insignificant, so it is usually ignored. The effects of some

stress mechanisms that cause aging are partially recoverable when the stress is removed for an appropriate time interval. Unfortunately, recovery from CHC-induced damage by removing or reducing the stress is insignificant so recovery from CHC is usually ignored.

2.2.2. Negative bias temperature instability(NBTI)

NBTI happens when the gate voltage of a PMOS transistor is negatively biased which occurs when the gate voltage is less than the source voltage. NBTI is due to a combination of hole trapping in the gate oxide and interface state generation under the stressed negative bias which is worse at high temperatures [27]. Due to the stressed conditions, Si-H bonds on the Si-SiO_2 interface are broken by energized holes, and the positive Si^+ ion is left when H_2 diffuses away. This Si^+ ion results in a continuous decrease of current and an increase of threshold voltage. In contrast to CHC, the generation of interface traps occurs over the whole channel surface. NBTI is independent of V_{DS} and channel length. However, threshold voltage itself is channel length dependent, so a small variation of NBTI effects with different lengths is still observable. Compared to the CHC effects, NBTI is partially recoverable when stress is removed. Some refer to this recovery as relaxation. It has been reported that for some devices, if the duty cycle of a stress condition is 50%, the degradation of threshold voltage due to NBTI is reduced by about one third compared to the degradation that would occur under constant static stress at the same level [28].

The R-D approach is also used for modeling the threshold voltage degradation due to NBTI. The time-dependent degradation under stress and relaxation from Wang [24] is given by

Under Stress:

$$\Delta V_{TH}(t) = \left[K_u (t - t_0)^{1/2} + \left(\Delta V_{TH}(t_0)\right)^{1/2n} \right]^{2n}$$
$$K_u = \left(\frac{qt_{ox}}{\varepsilon_{ox}}\right)^3 K_1^{\,2} C_{OX} (V_{GS} - V_{TH}) \sqrt{C} \exp\left(\frac{2E_{OX}}{E_{O1}}\right) \quad (1.22)$$

Under Relaxation:

$$\Delta V_{TH}(t) = \Delta V_{TH}(t_1) \left[1 - \frac{2\xi_1 t_e + \sqrt{\xi_2 C (t - t_1)}}{(1+\delta) t_{OX} + \sqrt{Ct}} \right] \quad (1.23)$$

where t_0 and t_1 are the start time of the stress and relaxation phases respectively. The parameters K_1, C and $E_{O1,}$ are the fitting parameters obtained from measurement results. The remaining parameters are as defined for (2.20). All model parameters and values [24] for a 65nm process are list in Table 2-8.

Table 2-8 Model parameters

Qi	C_{ox} (Vgs-Vth)	E_{OX}	(Vgs-Vth)/tox
Vdsat	$\frac{(Vgs - Vthedd + 2Vt) LeffEsat}{Vgs - Vtheff + 2Vt + AbulkLeffEsat}$	Em	(Vds-Vdsat)/l
Esi	$(\frac{2qN_b}{\epsilon_0 \epsilon_{si}} (\emptyset_s + V_t \exp\left(-\frac{2\phi_f}{V_t}\right)\left(\exp\left(\frac{\phi_s}{V_t}\right) - 1\right)))^{0.5}$		
C	Exp(-Ea/kT)/T0	γ	$\sqrt{2\epsilon q N_b}/C_{ox}$
Ea	0.49	tox(nm)	2.2
ϕ_f	$V_t \log(N_b/n_i)$	$K_1(C^{-0.5}nm^{-2.5})$	7.5
$T_0(s/nm^2)$	$1e^{-8}$	E_{01}(V/nm)	0.08
δ	0.5	E_{02}(V/nm)	0.8
$K_2(nmC^{-0.5})$	$1.7e^8$	E_{sat2}V/nm)	0.011
ξ_1	0.95	$\lambda(nm)$	7.8
ξ_2	0.5	α	5
$\varphi_{it}(eV)$	3.7	L(nm)	17
Vt(eV)	0.0259	Abulk	0.005
V_{fb}(V)	-1.05	m	1.6
		q	1.6e-9

2.2.3. Model validation

Though NBTI and CHC both contribute to time-dependent drift in the threshold voltage, NBTI effects are usually dominant in p-channel devices and CHC effects are usually dominant in n-channel devices [24]. In this section, the CHC model of (2.20) and the NBTI model of (2.21) will be used to model the threshold drift of n-channel and p-channel devices respectively in a 130nm process. Model parameters will be fit to the published measured data of Hoff [29] and Bhardwaj [28] to obtain predictive aging models for both n-channel and p-channel transistors.

The model of (2.20) was fit to the measured data of Fig. 5 in [29]. The fit parameters are given in Table 2-9 The corresponding model predicting the aging of V_{TH} for n-channel devices under different bias conditions is shown graphically in Fig. 2-15. The worst bias condition of CHC drift is when $V_{GS} \approx 0.5V_{DS}$.

Table 2-9 Fit parameters for CHC model of (2.20)

Vds(V)	**n'**	**K_2**
2.4	0.166	3.05
2.5	0.49	3.3
2.6	0.51	5.2

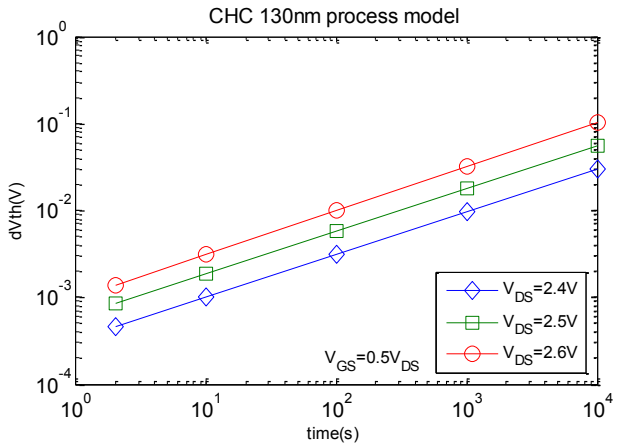


Fig. 2-15 NMOS Threshold voltage CHC aging characteristic in 130nm process

Correspondingly, the constant stress model of (2.21) was fit to the measured data of Fig. 4 in [28]. The fit parameters are given in Table 2-10. The corresponding model predicting the NBTI-induced aging of V_{TH} for p-channel devices under different E_{OX} conditions are shown graphically in Fig. 2-16 PMOS Threshold voltage NBTI aging characteristic in 130nm process. In applications where stress-relaxation cycles naturally occur, the aging effects should be significantly reduced.

Table 2-10 Fit parameters for constant stress NBTI model of (2.21)

Tox(nm)	2.6nm			
n'	0.25			
Temp(°C)	125C			
K1($C^{-0.5}nm^{-2}$)	8E4			
Eox(MV/cm)	9.1	8.0	6.9	5.7
Vgs-Vth(V)	2.366	2.08	1.794`	1.482

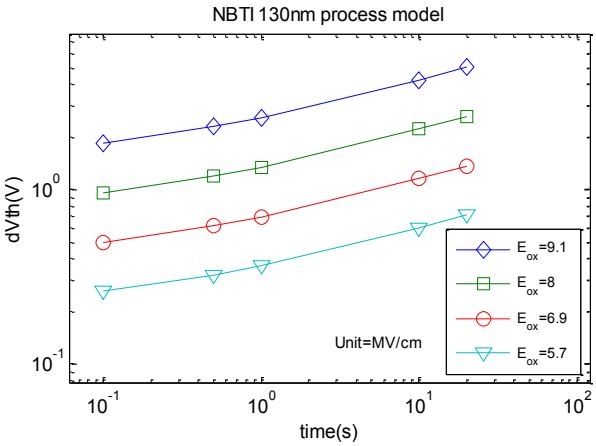


Fig. 2-16 PMOS Threshold voltage NBTI aging characteristic in 130nm process

2.2.4. Validation in five-transistor Widlar-type V_T -based temperature sensor

To predict the temperature sensor aging performance due to the shift of threshold voltage, CHC effects for NMOS transistor and NBTI effects for PMOS transistor will be considered using the models developed in the previous section. Threshold voltage shifts at particular time points were predicted from these models. The threshold voltage in the model file for Spectre was then modified by changing the threshold voltage to predict the aging performance of the temperature sensor.

In this work, several different temperature sensors were considered. For the purpose of predicting aging performance of the temperature sensor, the simple 5T temperature sensor of Fig. 2-17 was used as an example. This 5T temperature sensor was designed in a 130nm process and its operating points at the initial design stage are shown in Table 2-11.

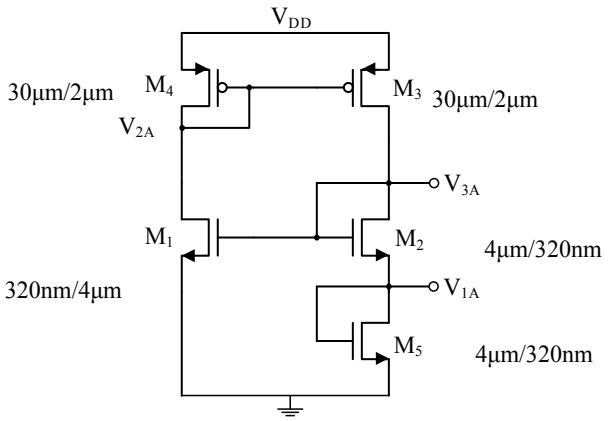


Fig. 2-17 Five-transistor Widlar-type temperature sensor test design in 130nm process

Table 2-11 Operating condition of 5T temperatures sensor in 130nm process

	Temp=27C	*VGS(V)*	*VDS(V)*	*VT(V)*
NMOS	*M1*	*0.674*	*0.9*	*0.1338*
	M2	*0.3635*	*0.3635*	*0.309*
	M5	*0.31*	*0.31*	*0.249*
PMOS	*M4*	*0.3*	*0.3*	*0.238*
	M3	*0.3*	*0.525*	*0.238*

The aging-induced error on the temperature sensor will now be determined. The shift in the output of the temperature sensor after 1 year at temperatures around 27°C is shown in Fig. 2-18. The overall voltage shift is about 0.0045mV at 27°C. With a temperature coefficient of this temperature sensor of 2.25mV/°C, the aging-induced degradation will cause a temperature error of only 0.002°C. Though Fig. 2-15 shows the shift only around 27°C, the temperature error due to aging will be approximately the same throughout the entire temperature range of the temperature sensor. Though this analysis was for this specific 5T temperature sensor, the aging characteristics should be negligible for the other temperature sensors considered in this work as well.

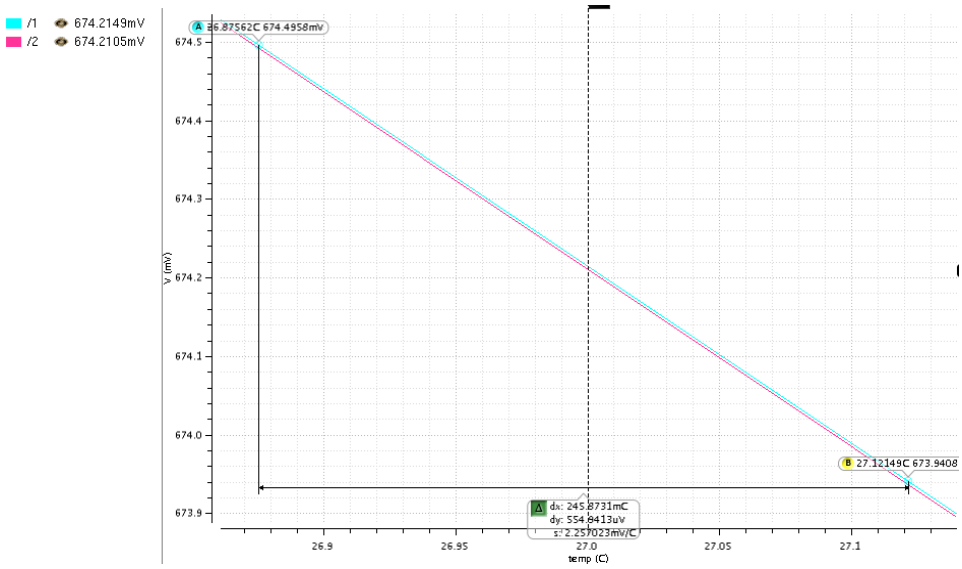


Fig. 2-18 Five-transistor Widlar-type temperature sensor output shift due to aging

2.2.5. Conclusion

The calculation and simulation results show that the aging of threshold voltage will not cause serious aging problem for the V_{TH}-based temperature sensors. The aging models were based upon the assumption of constant stress. Though not critical, a significant reduction in the aging characteristics will be realized if the NBTI recovery effect is included. Essentially all of the temperature sensors discussed in this dissertation operates very fast so likely a 1% or lower duty cycle will be adequate for measuring temperature. If a 1% duty cycle is used for the temperature sensor in power management applications, the drift due to CHC is becomes 1% of the static shift, and for NBTI, due to the fact of recovery, the shift will be less than 1% of the static shift. Table 2-12 shows the voltage drift under different duty cycles and usage time.

Table 2-12 Threshold voltage shift under normal condition

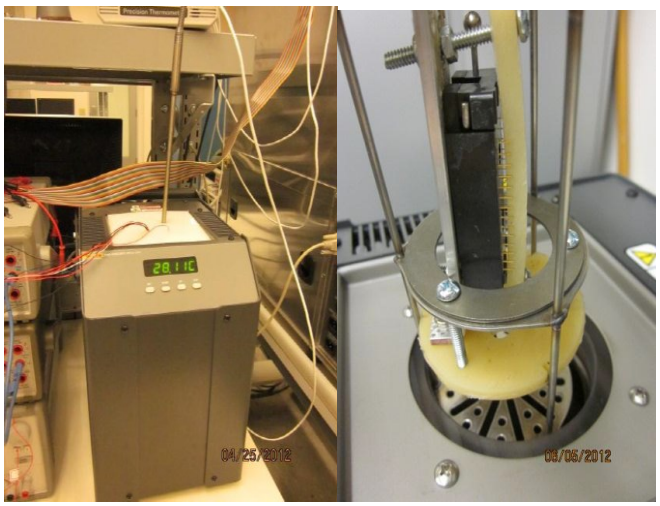
		100% DC@1yr	1% DC@10yr
NMOS	M_1	2.48×10^{-10} V	7.038×10^{-9} V
	M_2	2.27×10^{-23} V	6.456×10^{-22} V
	M_5	5.44×10^{-24} V	1.543×10^{-22} V
PMOS	M_3,M_4	0.078mV	1.47μV

2.3. Measurement Setup and Results

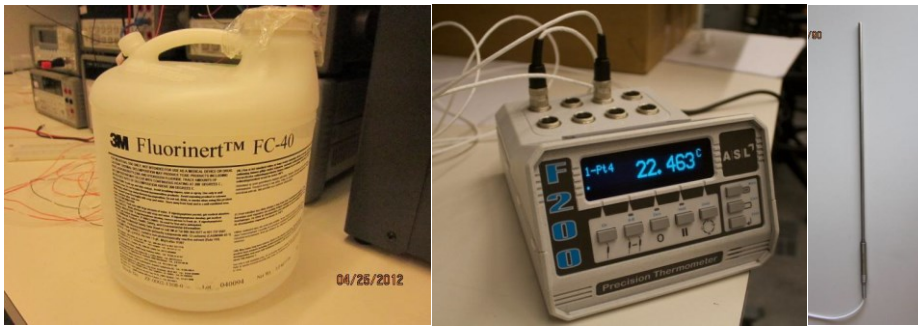
To verify the function and performance of fabricated chips, Fluke 7103 micro-bath in Fig. 2-19(a) with 3M™ Fluorinert™ electronic liquid FC-40 in Fig. 2-19(b) and T100-250-18 Platinum Resistance Thermometers (PRT) probe in Fig. 2-19(d) connected with F200 precision thermometer in Fig. 2-19(c) are used to test the chip. The designed chip with the socket and a PRT probe are bond together and put inside the micro-bath as shown in the right plot of Fig. 2-19(a) .

Fluke 7103 micro-bath can operate in the temperature range from -30°C to 125°C and meet ±0.25°C accuracy. The stability is ±0.03°C at- 25°C and ±0.05°C at 125°C. The thermal cycling rate is 2°C/min when heating up the temperature and 1°C/min when cooling down. The testing profile then can be programmable in the micro-bath to accommodate different requirements. A stir bar is included in the bottom of the micro-bath, and stirring makes temperature equilibrium all through the FC-40 Liquid. FC-40 is a stable single compound electronic liquid with 4E15Ω·cm resistivity and wide liquid range from -57°C ~165 °C which is suitable for the temperature sensor testing, and it is stable enough to insure the

repeatability of testing results. F200 thermometer withT100-250-18 PRT probe is using to be a temperature reference that target accuracy is ±25mK in the temperature range over -50°C to +250°C. An Agilent 6-digit multi-meter measures the output voltage of temperature sensors.



(a)



(a) (c) (d)

Fig. 2-19 Measurement equipment and setup configuration (a) Fluke 7103 micro-bath and socket installation (b) 3M^{TM} Fluorinert^{TM} FC-40 (c) F200 precision thermometer (d) T100-250-18 PRT

By recording the temperature information from PRT and the voltage results from multi-meter at the same time, the measure results of chip output and thermometer are compared to evaluate the performance of the designed circuit, and the temperature coefficient and accuracy can be evaluated.

Testing results emphasis on the application of power/thermal management which requires large amount temperature sensor strategically distributed on the chip. Throttling often is based upon a single predetermined temperature trigger, and for the safe operation, the temperature range is usually around 60°C~90°C. One testing profile is provided below in the Fig. 2-20, a ramp and soak temperature profile is given to the micro-bath. Starts from 50°C, and ramps up to 60°C, soaks for 2 hours, ramps up to 70°C, and repeat the process till 100°C. Since the micro-bath takes 5 minutes to heat up 10°C, the total testing period will be about 8.5 hours. This profile is used for TSMC 180nm process chips, and a similar but with different soaking temperature and time will be used for IBM 130nm process chips.

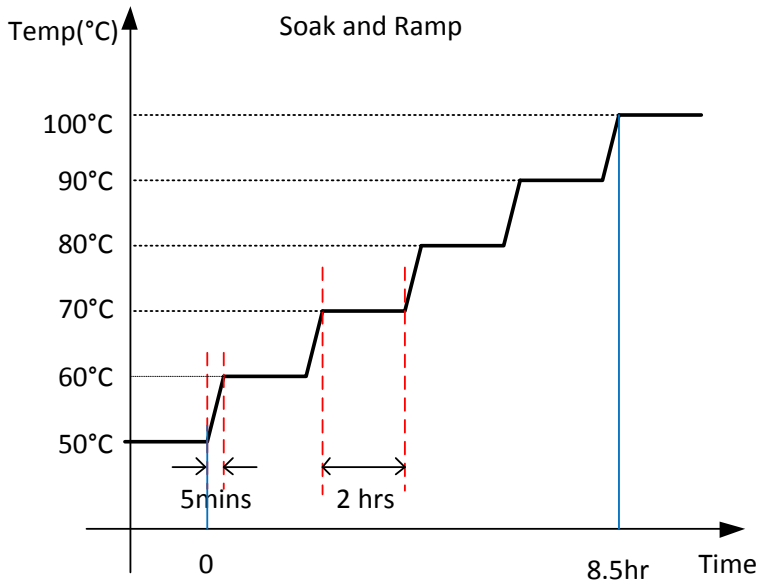


Fig. 2-20 Temperature control profile

Non-cascode 5T Widlar-type and cascode 4T dual-threshold temperature sensors with analog output are designed in TSMC 0.18 μm and IBM 0.13 μm process respectively and fabricated in three different runs.

2.3.1. Measurement resutls of 5T V_T based temperature sensor

The proposed 5TIW VTH-based temperature sensor with the start-up circuit is designed and fabricated in TSMC 0.18µm one-poly-six-metal (1P6M) CMOS process. Design size is listed in the Table 2-1 Design size of 5T Widlar-type temperature sensor and die photograph in two different runs are shown in Fig. 2-21. The total area for the single sensor is 15µm×24µm.

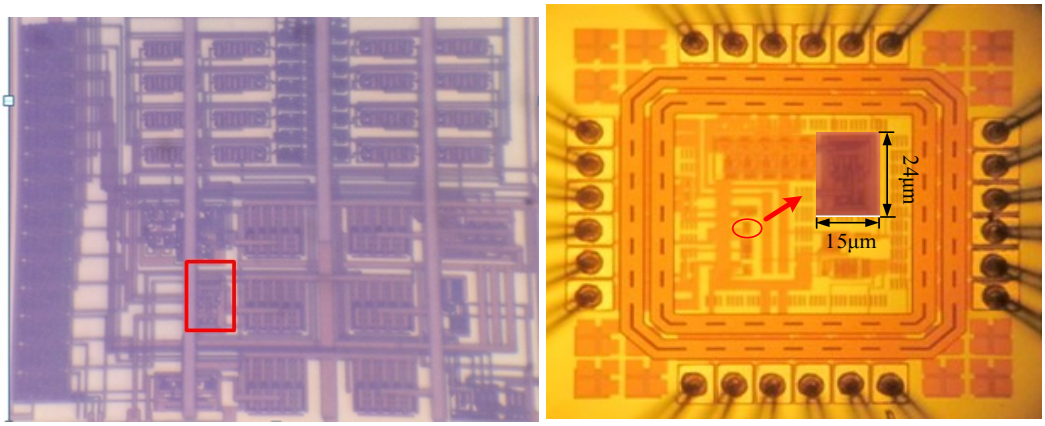


Fig. 2-21 Die photo of proposed temperature sensor

Nine Chips of 5-transistor inv-Widlar-based temperature sensors from two TSMC 0.18 µm fabrication runs are tested every 10°C from 60°C to 90°C in order to evaluate the performance. Fig. 2-22 shows the measured output voltages at each 10°C temperature from 60 °C to 90 °C. Due to the process variation, voltage offsets are included in the output voltages from the 9 sensors. The solid lines and dashed lines represent chips from different fabrication runs and reflect a shift in the nominal threshold voltage between the two runs.

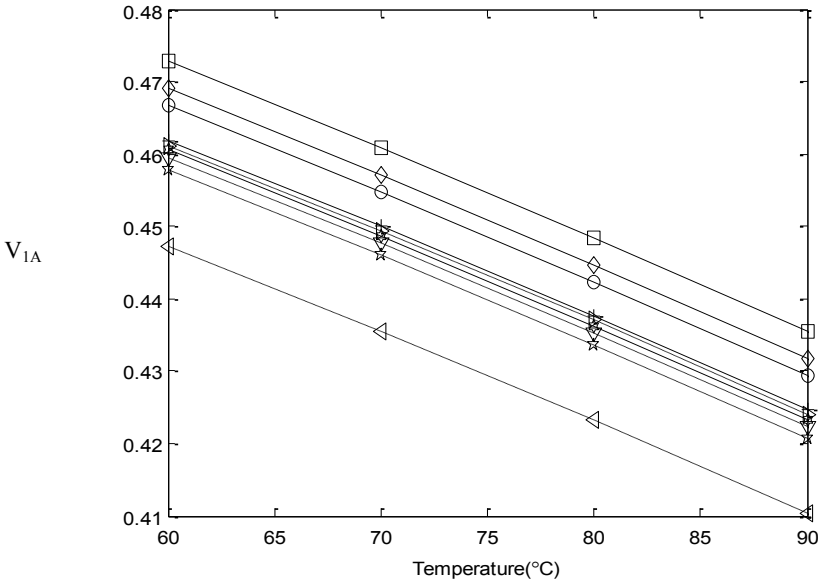


Fig. 2-22 Measurement results of proposed 5T temperature sensor output of nine-chips

The outputs of all nine chips were calibrated at a single temperature of 80°C using a simple level shift operation and batch slope calibration where the "batch" slope was obtained from devices from both batches. Calibrated results are shown in Fig. 2-23 which shows good accuracy and linearity over the target operating range. The temperature sensitivity is 1.2mV/°C. The temperature error from the batch fit line is a measure of the temperature error of this sensor and is shown in Fig. 2-24. It can be observed that the temperature error is within the range between -0.2°C to 0.6°C. The error distributions spread according to temperature difference between trigger the temperature defined by customers and calibration point. The more closed to calibration point, the smaller temperature error is. Such a one-point calibration is suitable for an actual application because it requires few setup transactions and also low cost.

A batch slope/curvature error correction was also implemented. In this case, the average curvature from all 9 chips from the two process runs was calculated. The residual error is shown in Fig. 2-25 where solid lines refer to devices from one process run and

dashed lines refer to devices from the other process run. Compared with just batch slope calibration, the accuracy is improved from [-0.2°C, 0.6°C] to [-0.1°C, 0.1°C]. From Fig. 2-25, it also can be observed that there is some difference between the curvatures of the two process runs. If batch calibration for slope and curvature were based upon a single process run rather than by merging sampled data from two process runs, some additional improvements in accuracy can be expected. And the result is in Fig. 2-26. It is, however, premature to predict the accuracy achievable with this single-point calibration since the number of samples in each process run is small and since we have samples from only two process runs. The power consumption is 95μW with 1.8V supply at 27°C.

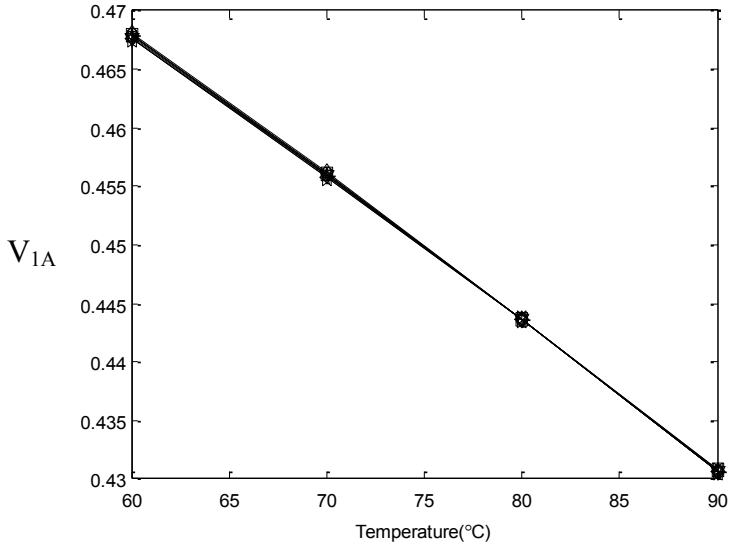


Fig. 2-23V_{1A} after one point calibration

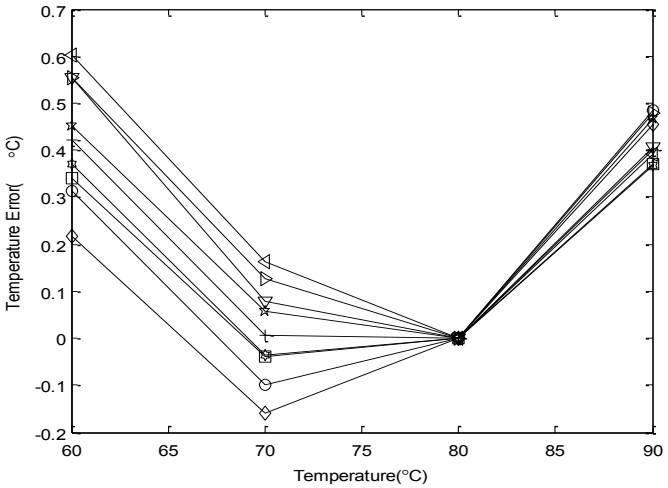


Fig. 2-24 Temperature Error of V_{1A} after one point batch slope calibration

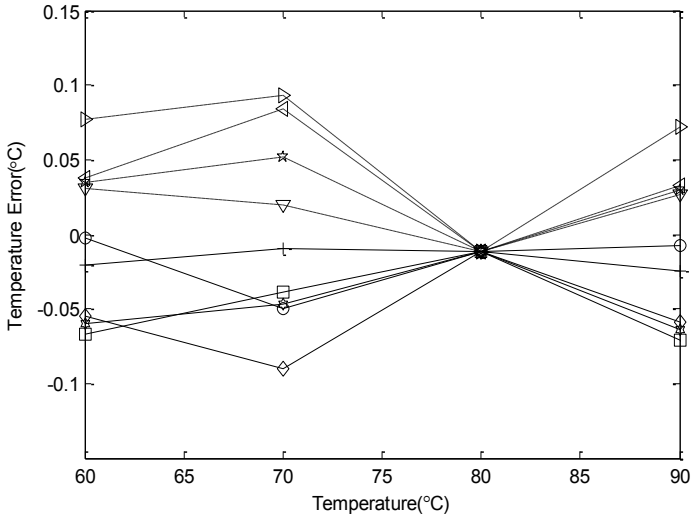


Fig. 2-25 Temperature error of V_{1A} after one point calibration and batch slope/curvature calibration

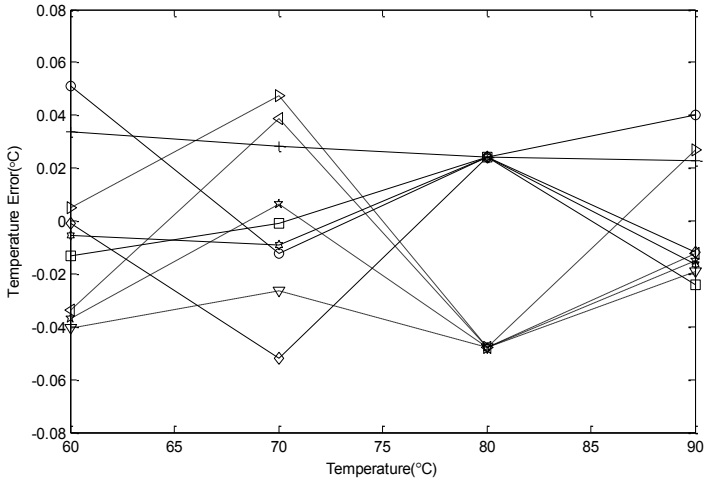


Fig. 2-26 Temperature error of V_{1A} after one point and batch slope/curvature (from separated process) calibration

2.3.2. Measurement results for Dual-threshold NTC temperature sensor

The 4T V_T based temperature sensor with cascode current mirror to increase the output conductance is designed in 0.13μm process, and the design parameter is listed in Table 2-6. Five chips in a lot are tested. The chip is soaked for one hour every 5°C over 60°C~90°C temperature range, and the voltage output of each chip for each soaked temperature is shown in Fig. 2-27. The measurement results show good consistency and linearity over different chips.

After one point and batch slope calibration at 75°C(without curvature calibration), the sensor achieved -0.18°C ~0.13°C temperature error as shown in Fig. 2-28. With ±10% supply change, the sensor output voltage changes ±0.365%. Compare to the five-transistor Widlar-type results in Fig. 2-24, Cascode dual-threshold shows better linearity while both results are trimmed with one point and batch slope calibration. This demonstrated that by increasing the output impedance, the second-order nonlinearity is reduced by a rational

amount. The power consumption is 60μW with 1.2V power supply at 75°C and the single sensor area is 1258 μm^2.

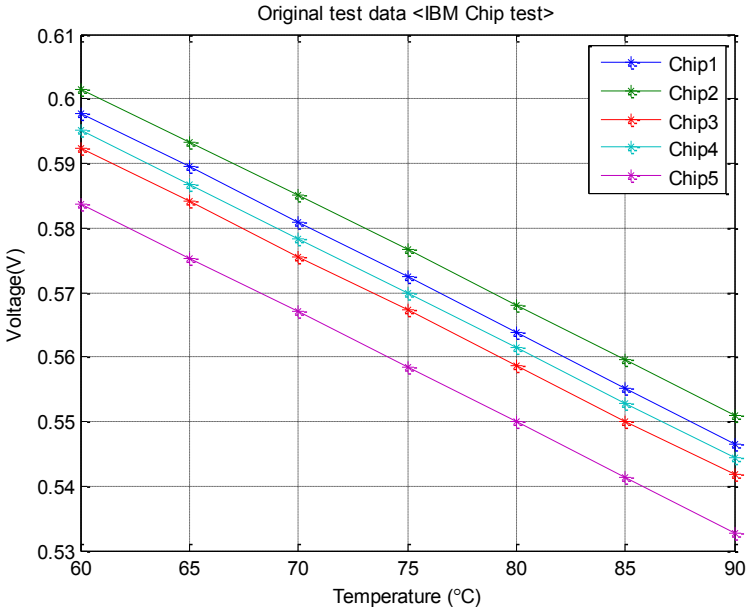


Fig. 2-27 Measurement output voltages for 4T temperature sensor in 60 ºC ~90 ºC temperature range

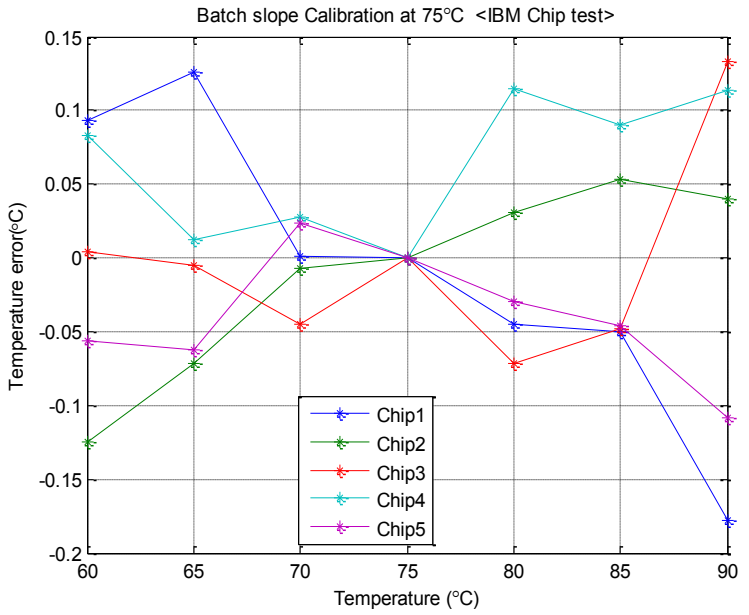


Fig. 2-28 Temperature error of V1B in 4T temperature sensor after one point batch slope calibration

2.4. Conclusion of temperature sensor design with analog output

This chapter focuses in the design of temperature sensors with analog output using CMOS threshold voltage. Various structures are designed and fabricated to show the pro and cons of each structure. Complete structure analysis has been done include large-signal and small-signal analysis to discuss the stability and startup issues. All designs are prove to be stable and start-up properly.

Transistor lifetime and the CHC and NBTI effects on threshold voltage degradation is also discussed in this thesis, and based on mathematical and simulation results, we also prove that the threshold voltage degradation in our temperature sensor is insignificant. Note that the lifetime and reliably of the circuit design is critical yet very few paper mention this problem and very few of them have complete analysis to their circuit.

This thesis also includes a dedicated testing plan which gives a stable measurement environment to minimize the testing error. With the repeatable measurements, the results show that the Dual-threshold temperature sensor provide ±0.1°C accuracy with one-point calibration cost only 60 μW power consumption. Compare to our 5TIW Temperature sensor, although the area costs four times bigger, the need of calibration is less which save more costs. Compare with [11] Yang, our sensor consume more power and area; however, their circuit is not completed with the bias circuitry, it cannot operate standalone, yet with huge inaccuracy. Compare to the other analog temperature sensor, we provide better accuracy with comparable power and area.

Table 2-13 Temperature sensor with analog output performance summary

Sensor	[3] Shor ISSCC 2012	[4] Pertijis JSSC 2005	[7] Souri JSSC 2011	[8] Chen JSSC 2005	[11] Yang ISSCC 2014	[12] Law JSSC 2010	[14] Szekely TVLSI 1997	[30] Sasaki TSM 2008	[31] Jawed Microelectronic J. 2012	This Work 5T	This Work 4T
Type	BJT	BJT	BJT	Delay	V_T	weak	V_T/μ	V_T	V_T/μ/Res	V_T	V_T
Process (nm)	32	700	160	350	65	180	1000	90	250	180	130
Supply (V)	-	3.3	1.6	3.3	0.6	0.5/1	5	1	2	1.8	1.2
Power[1] (μW)	-	-	-	-	0.92	-	100	25	55	95	60
Power[2] (μW)	3780	247.5	7.4	10 2s/s	-	0.119 333s/s	-	-	-	-	-
Area[1] (μm^2)	11000	-	-	-	279	-	3000	48[3]	340[3]	360	1258
Area[2] (μm^2)	20000	4500000	120000	175000	-	41600	-	-	-	-	-
Error (◦C)	-0.8~1.4	±0.1	±0.2	-0.7~0.9	-3.4~3.2	-0.8~1	±1	-1~0.8	±0.2	±0.1	±0.1
Calibration	2	-	1	2	1		-	2 point	-	2	1
Temp (◦C)	20~100	-55~125	-30~125	0~100	0~100	-10~30	10~100	50~125	-100~200	60~90	60~90

[1] Analog sensor only
[2] Sensor with readout
[3] Exclude all biasing circuitry

CHAPTER 3 TEMPERATURE-TO-DIGITAL CONVERTER

In this chapter, a new approach of temperature to digital converter (TDC) design is introduced that offers potential for significant reductions in area, reductions in power dissipation, and improvements in performance when compared with the standard approach to the design of integrated temperature to digital converters. The standard approach to building TDCs is shown in the Fig. 3-1. With the standard approach, a temperature sensor and three ancillary blocks; a signal conditioner, a reference generator, and an analog to digital converter (ADC) are required. The quantity X_{SIG} can be a voltage, current, time, or period, and depends on the specific architecture used in the design. However, irrespective of the specific details, the performance is limited by that of these additional components. The ADC consumes significant power and area and requires a rather significant design effort. The ADC also needs a reference signal and good supply-insensitive reference generators, such as the standard bandgap structures, consume significant power and area. The inherent temperature dependence of the output of a bandgap reference generator and ADC also affects the overall performance.

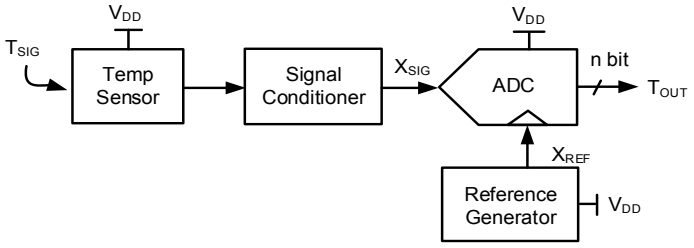


Fig. 3-1 Existing digital temperature sensor architecture

A binary temperature monitor that is used in the proposed approach is depicted in Fig. 3-2 binary temperature monitor contains a temperature sensor core and a simple comparator.

Unique to this binary temperature monitor are two analog outputs, V_1 and V_2, both of which contain temperature information. But critical to this binary temperature monitor is a requirement that the temperature information in V_1 and V_2 be embedded in "fundamentally different" ways. In this structure, an n-bit binary code is fed into the temperature sensor. This controls n switches which adjust the temperature sensor that, in turn, affects V_1, V_2, or both V_1 and V_2.

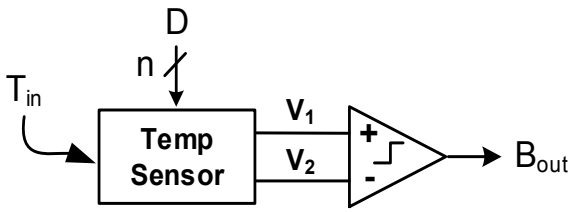


Fig. 3-2 Proposed binary temperature monitoring system

A conceptual depiction of properties of "fundamentally different" relationships between the temperature dependence of V_1 and the temperature dependence of V_2 that would be suitable for the binary temperature monitor is shown in Fig. 3-3 where in this depiction $V_1(T)$ is independent of the digital input D. But, as the digital input is varied from D=(00000) to D=(11111), the temperature dependence of the voltage $V_2(T)$ varies. The intersection of V_1 and V_2 for any value of $D_k(d_{k5},d_{k4},d_{k3},d_{k2},d_{k1})$ is denoted as T_k. In this depiction, there is a unique and monotone relationship between the Boolean signal $D_k(d_{k5},d_{k4},d_{k3},d_{k2},d_{k1})$ and temperature T_k. If this relationship is known, the Boolean signal D_k can be viewed as a digital representation of the temperature T_k.

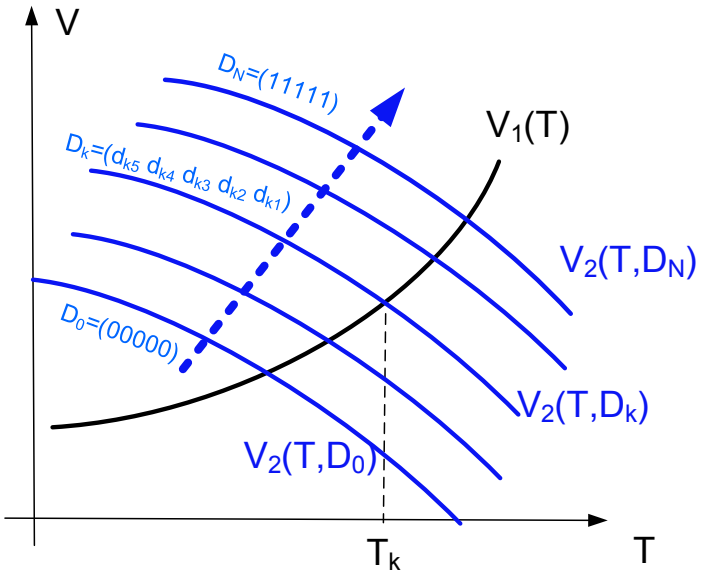


Fig. 3-3 Conceptual relationships between V_1 and V_2

In a specific implementation of the proposed approach discussed later in this section, the n switches will control the effective size of one of the transistors internal to the *Temp Sensor*. This size adjustment changes one of the output voltages. The digitally controlled binary temperature monitor can work as a temperature trigger with a fixed Boolean input where the Boolean input *D* determines the trigger temperature. When serving as a temperature trigger, the output of the comparator changes states at the trigger temperature determined by the D input.

The "fundamentally different" relationships between V_1 and V_2 that are required for the binary temperature monitor can now be defined to be a circuit that has the following three properties:

Property 1: For each Boolean signal D_k there exists a unique temperature T_k where $V_1(T_k)=V_2(T_k)$

Property 2: The relationship between D_k and T_k, denoted as $D_k(T_k)$, is monotone.

Property 3: $V_1(T)$ and $V_2(T)$ are continuous functions of T with the properties that for any D_k and for any $T_k<T<T_{k+1}$

$$V_1(T_k)>V_1(T)>V_1(T_{k+1}) \text{ if } V_1(T_k)>V_1(T_{k+1})$$

$$V_1(T_k)<V_1(T)<V_1(T_{k+1}) \text{ if } V_1(T_k)<V_1(T_{k+1})$$

$$V_2(T_k)>V_2(T)>V_2(T_{k+1}) \text{ if } V_2(T_k)>V_2(T_{k+1})$$

$$V_2(T_k)<V_2(T)<V_2(T_{k+1}) \text{ if } V_2(T_k)<V_2(T_{k+1})$$

With these three properties, the Boolean signal D_k can be viewed as a digital representation of the temperature T_k.

Since it is assumed that Boolean signal D_k in the binary temperature monitor is a digital representation of the temperature T_k, a TDC can be realized by adding a digital feedback block as shown in Fig. 3-4 where the feedback block will adjust the Boolean signal *D,* based upon the comparator output B_{OUT}. This adjustment will force $V_1(T)$ to be approximately equal to $V_2(T)$ and when this occurs, the Boolean signal D_k will be a digital representation of the temperature T. The control block can be quite simple and one implementation could be with little more than an up/down binary counter and a small amount of control logic.

Although it might appear that the comparator and logic block combination is just another way of depicting a specific type of ADC that uses only a single comparator, such as a sigma-delta or a successive approximation (SAR) architecture, in the proposed approach, there is no such digital to analog converter (DAC) in a feedback path and there is no voltage being generated that serves as an input to the ADC. Rather, the logic block itself will simply

reconfigure the temperature sensor in such a way that the input temperature is encoded in the digital output code.

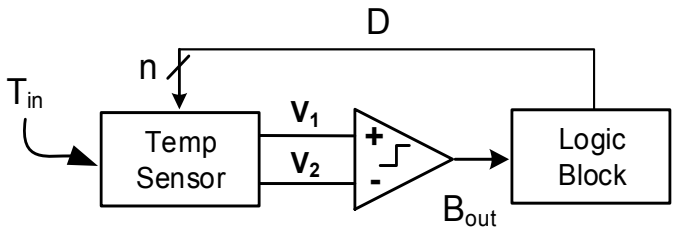


Fig. 3-4 Proposed direct temperature-to-digital converter

3.1. A TDC with Two NTC Voltages

In this section, a TDC based upon the architecture of Fig. 3-4 where the voltages V_1 and V_2 both have negative temperature coefficients (NTC) will be discussed. It is based upon an inverse Widlar bias generator where the bias voltage is generated with a separate dual threshold 4-transistor core temperature sensor. Since the design of the logic block is straightforward and the performance of the TDC is determined primarily by that of the binary temperature monitor of Fig. 3-4, emphasis will be placed at the transistor level on the binary temperature monitor with a behavioral description of the Logic Block.

3.1.1. Two NTC TDC structure

The schematic of a TDC with two NTC voltages is shown in Fig. 3-5 where it is assumed the Logic Block will generate the Boolean output D_{OUT} based upon the output of the comparator, B_{OUT}. The temperature sensor is comprised of a self-stabilized 4-transistor dual-threshold core and a current to voltage converter. Both the 4-transistor dual-threshold core and the current to voltage converter have enough headroom for full cascoding to minimize

power supply sensitivity. This Temperature Sensor Core typically does not require a start-up circuit. Although the actual implementation was fully-cascoded, for notational convenience, the basic operation will be described in the context of the non-cascoded structure of Fig. 3-5. Transistor M_2 in the core is a high V_T transistor. All other transistors are normal V_T transistors.

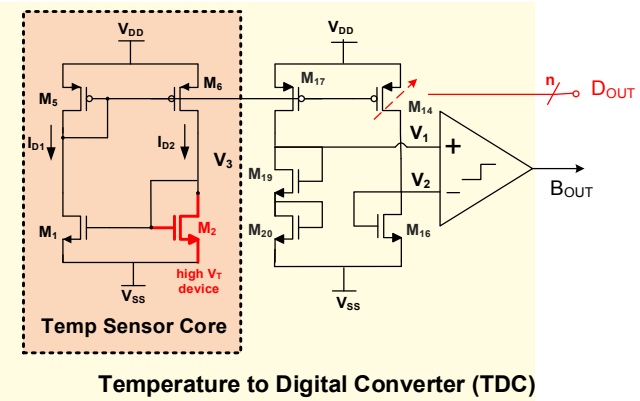


Fig. 3-5 Schematic of proposed direct temperature-to-digital converter

Ignoring the output conductance effects, assuming the M_5:M_6 current gain is one, and assuming the transistors can be characterized by the ideal square-law model, it follows that:

$$I_{D1} = \frac{\mu_n C_{ox}}{2} \frac{W_1}{L_1} (V_3 - V_{Tn1})^2 \tag{3.1}$$

$$I_{D2} = \frac{\mu_n C_{ox}}{2} \frac{W_2}{L_2} (V_3 - V_{Tn2})^2 \tag{3.2}$$

$$I_{D1} = I_{D2} \tag{3.3}$$

Solving equations (3.1)–(3.3), an expression for the output voltage V_3 of the *Temp Sensor Core* can be written as,

$$V_3 = \frac{\sqrt{W_1/L_1}}{\left(\sqrt{W_1/L_1} - \sqrt{W_2/L_2}\right)} V_{Tn1} - \frac{\sqrt{W_2/L_2}}{\left(\sqrt{W_1/L_1} - \sqrt{W_2/L_2}\right)} V_{Tn2} \tag{3.4}$$

It can be observed that the output voltage of this temperature sensor core is a linear combination function of two threshold voltages which are nominally both nearly linearly dependent on temperature. With a similar analysis, it can also be shown that the voltages V_1 and V_2 are nearly linearly dependent upon temperature but the temperature dependent slope and offset of V_1 and V_2 will be different.

Transistor M_{14} is a Boolean-controlled transistor. The effective size of transistor M_{14} is controlled by switching in additional "fingers" based upon the Boolean code D_{OUT}. Details of the switch using binary weighted finger sizes are shown in Fig. 3-6 for a 4-bit implementation. The left-most transistor is of fixed size and the remaining transistors are controlled by D_{OUT}. The relative size of M_{14_FIX} an $M_{14[0]}$ sets the resolution.

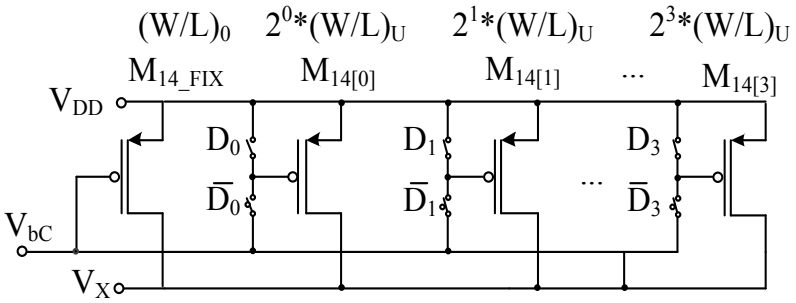


Fig. 3-6 Boolean controlled transistors

The performance characteristics of the comparator are not critical except for a low offset voltage. A simple latch comparator that has been used in a prototype implementation is shown in Fig. 3-7. It is comprised of a differential comparator followed by the cross coupled latch. If M_1 and M_2 are nominally matched and M_3 and M_4 are nominally matched, the input-

referred offset is dominated by the random mismatch in the n-channel and p-channel threshold voltages and is given the expression [32]

$$V_{OS} \cong V_{Tn1} - V_{Tn2} + \frac{V_{ovN}}{|V_{ovP}|}\left(V_{Tp3} - V_{Tp4}\right) \tag{3.5}$$

where V_{ovN} is the nominal excess bias voltage of M_1 and V_{ovP} is the nominal excess bias voltage of M_3.

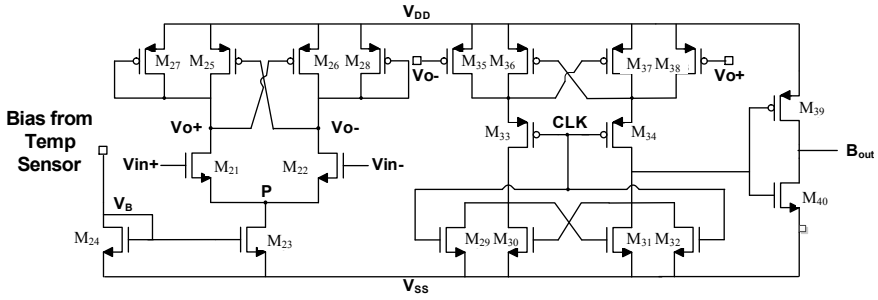


Fig. 3-7 Three-stage latch comparator

The offset voltage given in (3.5) is a random variable which, in turn, is a function of the four random variables V_{Tn1}, V_{Tn2}, V_{Tp3} and V_{Tp4}. If gradient effects are neglected or if common-centroid layouts are used for M_1 and M_2 as well as for M_3 and M_4 to eliminate gradient effects in the offset voltage, the threshold voltages of all four transistors are uncorrelated and are approximately Gaussian and characterized by their standard deviations. If follows that V_{OS} is also Gaussian. The threshold voltages V_{Tn1} and V_{Tn2} will have identical distributions as will the threshold voltages V_{Tp3} and V_{Tp4}. It directly follows that the mean of V_{OS} is zero and the standard deviation is given by the expression

$$\sigma_{OS} \cong \sqrt{2\sigma_{V_{Tn1}}^2 + 2\left(\frac{V_{ovN}}{|V_{ovP}|}\right)^2 \sigma_{V_{Tp3}}^2} \tag{3.6}$$

The standard deviation of V_{Tn1} and V_{Tp3} are given by the expressions

$$\sigma_{V_{Tn1}} = \frac{A_{V_{Tn}}}{\sqrt{W_1 L_1}} \qquad \sigma_{V_{Tp3}} = \frac{A_{V_{Tp}}}{\sqrt{W_3 L_3}} \tag{3.7}$$

where A_{VTn} and A_{VTp} are process related constants [46]

Substituting from (3.7) into (3.6), we obtain the expression

$$\sigma_{OS} \cong \sqrt{2\frac{A_{V_{Tn}}^2}{W_1 L_1}\sigma_{V_{Tn1}}^2 + 2\left(\frac{V_{ovN}}{|V_{ovP}|}\right)^2 \frac{A_{V_{Tp}}^2}{W_3 L_3}\sigma_{V_{Tp3}}^2} \tag{3.8}$$

The quantities A_{VTn} and A_{VTp} can be expressed as

$$A_{V_{Tn}} \cong t_{ox}\sqrt[4]{N_{Bn}} \qquad A_{V_{Tp}} \cong t_{ox}\sqrt[4]{N_{Bp}} \tag{3.9}$$

where $N_{Bn\ and}$ N_{Bp} are the substrate doping concentrations of the n-channel and p-channel devices respectively. As shown in (3.8), the random input offset can be reduced by increasing the device sizes.

The input offset is also temperature dependent, and may contribute to a slope error in the digital code of the TDC but these minor variations can be compensated in the digital output with a batch slope calibration.

The offset analysis was based upon the assumption that gradient effects can be neglected. If gradient effects cannot be neglected, a common-centroid layout of M_1 and M_2 as well as a common-centroid layout of M_3 and M_4 is necessary to minimize the offset voltage of the comparator. With a single-temperature calibration, the offset at that temperature can be cancelled. If the offset voltage is problematic, an offset-cancelled comparator can be used to remove the effects of offset over a large temperature range.

3.1.2. Operation of the two NTC TDC

The operation of the TDC of Fig. 3-5 can best be described by considering the target temperature dependence of V_1 and V_2 as shown in Fig. 3-8. The circuit has been designed so that by changing the size of M_{14} with D_{OUT}, the temperature characteristics of V_2 shifts up and down. Since the slope of V_1 is different from that of V_2, the intersection point changes with both temperature and with the code D_{OUT}. By scanning digital codes at a constant temperature and monitoring he output of the comparator, B_{OUT} in Fig. 3-2, the digital code transition that corresponds to a change in state of the comparator can be determined. At that temperature, $V_1 = V_2$, so the digital code transition corresponding to that constant temperature is obtained. By repeating the process at different constant temperatures, a relationship between the Boolean transition codes and temperature is obtained. Thus, the Boolean code at transition is a representation of temperature. Once this relationship is known, the circuit can be used as a TDC by sweeping the digital input code until a transition occurs at the output of the temperature. The digital code corresponding to the comparator transition is thus a digital representation of the temperature. It can actually be shown that the circuit can be designed so that the relationship between digital code and temperature is quite linear though nonlinearity can be readily compensated for in the digital domain if the relationship is known. From the plots in Fig. 3-8 that show how V_1 and V_2 vary with temperature, a plot of D_{OUT} vs T corresponding to the state change in the comparator can be readily obtained. Though the plot in Fig. 3-8 shows only four digital codes corresponding to a TDC with 2 bits of resolution, a larger number of bits of resolution of the TDC can be obtained by adding V_2 transfer characteristics for additional Boolean inputs.

For power management applications, the logic needed to adjust D_{OUT} can be a part the power management system and only digital signals are needed to interface between the TDC and the controller. In these applications, one power management logic unit can be used to adjust the D_{OUT} for a large number of TDCs on a chip and since only low-speed digital signals are needed to interface between the controller and the TDC, circuit noise will not play a major role in the performance of the TDC. Alternately, a simple up/down counter and a small logic circuit can be located near the TDC to realize a self-contained temperature sensor with Boolean output.

When used as a temperature trigger, the digital code D_{OUT} can be set at a fixed value corresponding to the desired trigger temperature and the comparator output will serve as a trigger signal to determine when the temperature exceeds the trigger temperature.

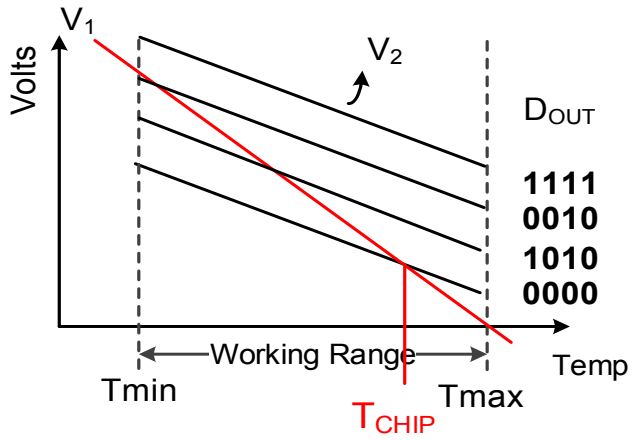


Fig. 3-8 Relationship between temperature and output code

3.1.3. Cascoded implementation of the TDC

If changes in supply voltage cause a differential signal to appear between nodes V_1 and V_2, this differential signal will result in a temperature error. To reduce the effects of supply voltage on V_1 and V_2, cascoding of the temperature sensor can be used. Since the

core temperature sensor is based upon a 4-transistor self-stabilized structure, full cascoding at even low supply voltages is possible. The fully cascoded TDC along with bias generators is shown in Fig. 3-9. As discussed for the non-cascoded structure, no start-up circuit is typically needed for the TDC.

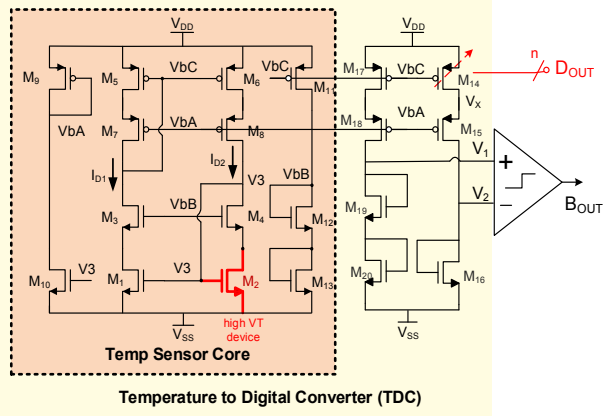


Fig. 3-9 Fully Cascoded TDC

3.1.4. TDC current mirror gain

Each D_{OUT} will generate different current mirror gains between the M_{17} branch and the M_{14} branch in Fig. 3-5. Assuming all transistors are operating in the saturation region and assuming the current mirror gains $M_{6:5}$ and $M_{17:5}$ are unity, the current mirror gain in the TDC when V_1=V_2 is given by the expression

$$K = \left(K_1 + K_2 \frac{V_{THN1}}{V_{THN1} - V_{THN2}} \right)^2 \tag{3.10}$$

where K_1 and K_2 are both positive and given by the expressions

$$K_1 = \frac{\left(W/L\right)_{16}}{\left(W/L\right)_{19}} + \frac{\left(W/L\right)_{16}}{\left(W/L\right)_{20}}, K_2 = \frac{\left(W/L\right)_{16}}{\left(W/L\right)_{2}} - \frac{\left(W/L\right)_{16}}{\left(W/L\right)_{1}}.$$

The threshold voltages V_{THN1} and V_{THN2} are assumed to be linearly dependent upon T and modeled by the expressions

$$\begin{aligned} V_{THN1} &= V_{THN10} + \gamma_1 T \\ V_{THN2} &= V_{THN20} + \gamma_2 T \end{aligned} \tag{3.11}$$

where $V_{THN10}<V_{THN20}$ and the temperature coefficients γ_1 and γ_2 are both negative. It can be shown that in most cases K is nearly linearly dependent on T as well and the slope of K is also negative.

Three potential problems can be identified that may render the TDC approach ineffective at sensing temperature. These three scenarios will now be discussed.

Scenario 1:

$$V_{THN1} = V_{THN2} \tag{3.12}$$

In this case, K will become ∞ thereby losing the ability to encode temperature in the Boolean representation of K.

Scenario 2,

V_{THN2} is a scaled version of V_{THN1}

$$V_{THN2} = \theta V_{THN1} \tag{3.13}$$

It follows that K can be expressed as

$$K = \left(\rho_1 + \rho_2 \frac{\theta V_{t1}}{\left(V_{t1} - \theta V_{t1}\right)} \right)^2 = \left(\rho_1 + \rho_2 \frac{\theta}{\left(1-\theta\right)} \right)^2 \tag{3.14}$$

Note that in this case, K is independent of T thereby also loosing the ability to encode temperature in the Boolean representation of K.

Scenario 3,

V_{THN2} differs a small amount from a scaled version of V_{THN1}.

That is,

$$V_{THN2} = \theta V_{THN1} + \varepsilon(T) \tag{3.15}$$

where for $T_{MIN}<T<T_{MAX}$,

$$|\varepsilon(T)| << V_{THN2}$$

In the third scenario, K is only weakly dependent upon T and large changes in K will occur for $T_{MIN}<T<T_{MAX}$.

A statistical model for transistors in a dual-VT process that includes the random variations in the temperature coefficients of the threshold voltages will now be developed. This will be useful for determining whether any of the three identified scenarios will limit the operation of the TDC.

It will be assumed that the two threshold voltages as given in (3.11) and repeated as (3.16) can be expressed as

$$\begin{aligned} V_{THN1} &= V_{THN10} + \gamma_1 T \\ V_{THN2} &= V_{THN20} + \gamma_2 T \end{aligned} \tag{3.16}$$

where the four quantities $\{V_{THN10}, V_{THN20}, \gamma_1, \gamma_2\}$ are independent of temperature. These quantities are process variables so they are random variables at the design stage. In Fig. 3-10 the probability density functions of V_{THN10} (denoted as f_1) and V_{THN20} (denoted as f_2) for two different scenarios that may occur in different processes are shown. In Fig. 3-10 (a), the two distributions show little or no overlap so the two threshold voltages, at least at very low temperatures, are statistically separated and Scenario 1 listed above is unlikely to occur. In Fig. 3-10 (b), the low threshold voltage, at least for very low temperatures, has a nonzero probability of exceeding the high threshold voltage and there is a nonzero probability that either Scenario 1 or Scenario 3 will occur. Though this argument was made at low temperatures, similar concerns exist at more normal operating temperatures when the statistical variations associated with the random variables γ_1, γ_2 are included.

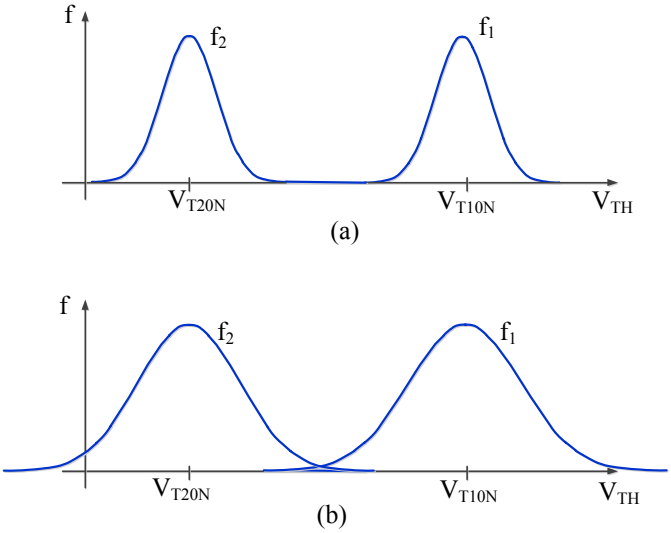
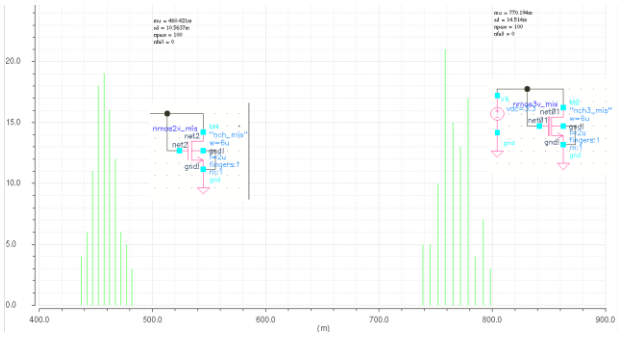


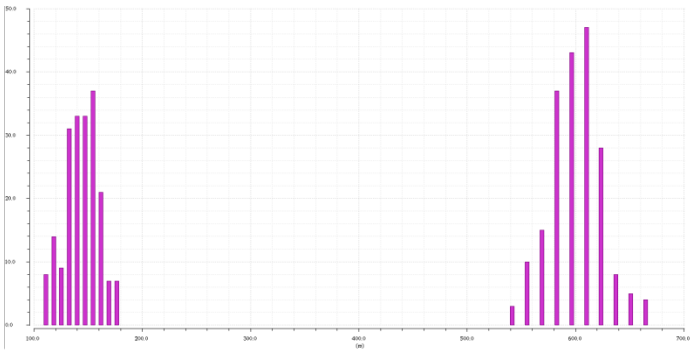
Fig. 3-10 Distribution of threshold voltages in a dual-threshold process

Monte Carlo simulations have been run in both 130nm and 180nm process with dual V_{TH} devices to assess the statistical variations of the threshold voltages. Unfortunately it is not clear whether good models for the statistical variation of the four random variables

$\{V_{THN10}, V_{THN20}, \gamma_1, \gamma_2\}$ and possibly their correlation are included in the statistical models available in PDKs for the processes but rather the threshold voltage at a given temperature was treated as a random variable. The histogram results of Monte Carlo simulations with both high and low threshold voltages for two different processes are shown in Fig. 3-11. As can be seen from these histograms, it appears that the corresponding probability density functions are void of overlap and actually the distribution functions are widely separated.



(a) Histograms of threshold voltages of two different devices in a commercial 0.18µ process



(b) Histograms of threshold voltages of two different devices in a commercial 0.13µ process

Fig. 3-11 Monte Carlo simulation of threshold voltages in dual-threshold process

(a)0.18µ process (b) 0.13µ process

However, dual-V_{TH} devices are not available in the all processes. Since the threshold voltage of MOS transistors exhibit significant length dependence for short devices, the concept of using different lengths to realize dual-threshold devices deserves attention.

Simulation results from a Monte Carlo analysis showing histograms of the threshold voltage of two devices with different nominal lengths are shown in Fig. 3-12. In these histograms, it can be observed that the lower threshold voltage can actually be larger than the higher threshold voltage so at least in the process considered here, it is not practical to obtain the dual thresholds needed for the design of the proposed TDC by changing the lengths of the transistors.

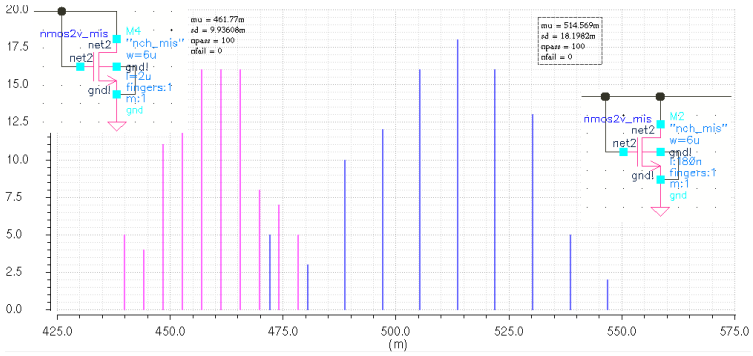


Fig. 3-12 Distribution of threshold voltages in a single-threshold process with different device length

Even if the threshold voltages are widely separated in a statistical sense, the conditions identified by Scenario 2 and Scenario 3 above where the threshold voltage of the high-threshold transistor is a scaled version or nearly a scaled version of the threshold voltage of the low threshold transistor must be avoided and to address this concern both the random nature of $\{V_{THN10}, V_{THN20}\}$ as well as that of $\{\gamma_1, \gamma_2\}$ must be considered. The γ-V_{THN0} plane is shown in Fig. 3-13 .The two black dots show the mean values the random variable pairs $\{V_{THN10}, \gamma_1\}$ and $\{V_{THN20}, \gamma_2\}$. The purple dashed regions represent the 3σ boundaries of these random variables which will be boxes if the corresponding random variables are uncorrelated. In the plot, it has been assumed that there is no overlap of the 3σ

boundaries of these two random variables. These 3σ boundaries may denote the process corners for these random variables and the points in the plane where the black dots are located are the TT values for these variables. Also shown on the plot are some purple X symbols. Two of these are paired to denote what is likely the FF corner and two are paired to denote the SS process corner. m_1, m_2,...m_k denote the slopes, in increasing order, of a set of lines that pass through the origin in the V_{THN0}-γ plane. An actual high-threshold transistor and low threshold transistor can be represented by samples of these four random variables as two dots in the γ-V_{THN0} plane. If two dots are on the same line, then it will satisfy Scenario 2 above, V_{THN2}=θV_{THN1}, and the circuit will lose the gain-temperature relationship. And if the two dots are close to the same line, then it will satisfy Scenario 3 above and the change in gain with temperature will be too large to make proposed TDC practical.

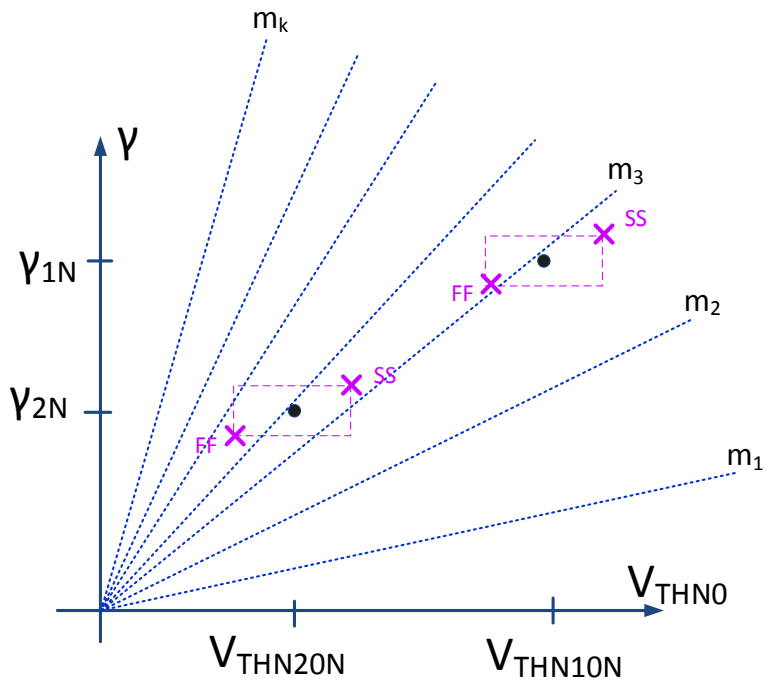


Fig. 3-13 Distributions of V_{THN0} and γ

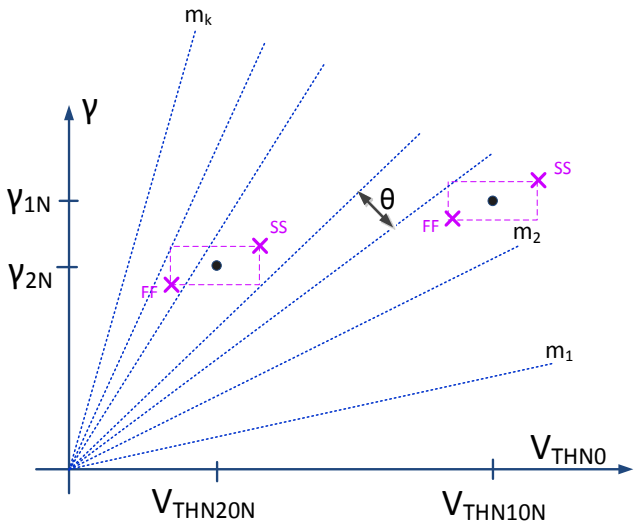
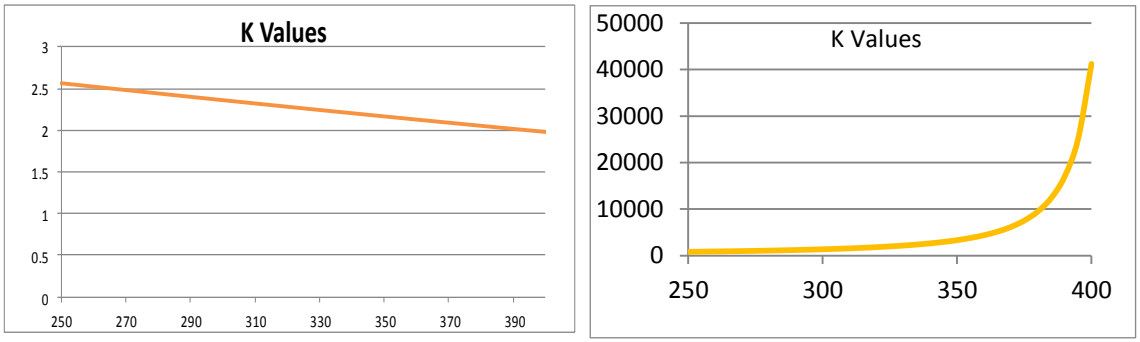


Fig. 3-14 Statistical separation of high and low threshold voltages

From Fig. 3-13, the concept of statistical separation of the high and low threshold voltages in the context of the random variables $\{V_{THN10}, V_{THN20}, \gamma_1, \gamma_2\}$ can be stated. Specifically, the two ordered random variable pairs $\{V_{THN10}, \gamma_1\}$ and $\{V_{THN20}, \gamma_2\}$ are widely separated if the angle θ in Fig. 3-14 that separates the worst-case statistical boundaries of the two distinct ordered pairs is sufficiently large.



(a) (b)

Fig. 3-15 TDC gain and temperature relationship

In Fig. 3-15 (a), the normal operation of the TDC showing the relationship between gain K and temperature when the threshold voltages have enough statistical separation is shown. With normal operation, the TDC gain is linear dependent on temperature. And if two threshold voltages have a relationship where the angle θ as shown in Fig. 3-14 is too small, the gain will become exceedingly large and highly nonlinear as shown in Fig. 3-15(b).

Though the concept of statistical separation is readily shown in Fig. 3-15 from a practical viewpoint it is often difficult to obtain the statistical information relating the random variables $\{V_{THN10}, V_{THN20}, \gamma_1, \gamma_2\}$ since a process delivery kit (PDK) is often missing this information. There is little evidence that those characterizing a semiconductor process have placed a strong emphasis on characterizing these parameters.

Fig. 3-16 shows the process simulation results in IBM process. The device type and sizes used for simulation are M1 and M2 in TDC circuit. The orange dot is High-V_{TH} device and blue dot is nominal V_{TH} device, from the result, the angle θ is large than 0. However, as mentioned above, statistical information is not complete for the PDK. For this particular process, the nominal-V_{TH} device has the statistical parameter for both gamma and V_{THO}, yet High-V_{TH} device only contain V_{THO} variation.

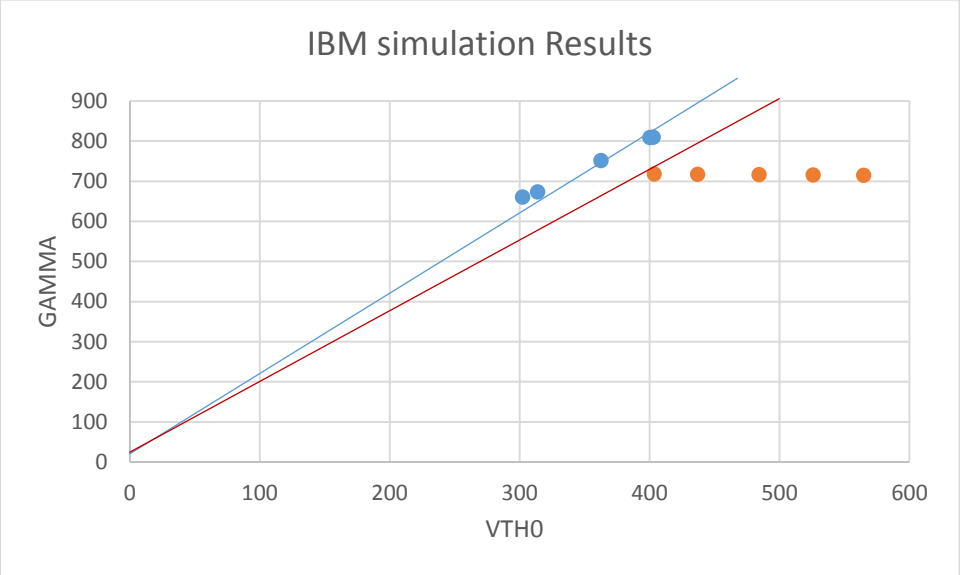


Fig. 3-16 Statistical separation Simulation Results for TDC design circuit

3.2. Improved TDC with NTC and PTC Voltages

In the previous TDC design, the two voltages generated from the temperature sensor that are inputs to the comparator are both NTC voltages. The slopes (on the temperature axis) are limited by the process since they are functions of the threshold voltages. There are two issues that must be addressed in the proposed TDC design approach. First, based on the analysis in the previous section, when the two ordered random variable pairs $\{V_{THN10}, \gamma_1\}$ and $\{V_{THN20}, \gamma_2\}$ are too close to each other in a statistical sense, the digitally controlled current mirror gain $K_{5:14}$ will be unacceptably large and highly nonlinear. The second issue that is of concern with this design is that the required difference between V_1 and V_2 can be quite small resulting in the requirement of a low offset comparator.

Both concerns can be reduced or eliminated by introducing a positive temperature coefficient (PTC) voltage in the temperature sensor thereby making the change in the difference between V_1 and V_2 with temperature much larger. This will reduce the low offset

voltage constraints on the comparator. In Fig. 3-17 (a) a scenario of comparing a fixed NTC sensor and a controllable NTC (FNCN) sensor is shown. Correspondingly, the outputs of a fixed NTC and a controllable PTC (FNCP) temperature sensor are shown in Fig. 3-17(b). The characteristics of a sensor cell that has both a digitally controllable NTC output and a digitally controlled PTC output are shown in Fig. 3-17(c). It can be observed from the V_1-V_2 characteristics of the FNCP sensor depicted in Fig. 3-17(b) that V_1 and V_2 form a larger angle at their intersection points than was obtained at the intersection points of the FNCN sensor depicted in Fig. 3-17(a). The larger intersection angle reduces the offset voltage requirements of the comparator.

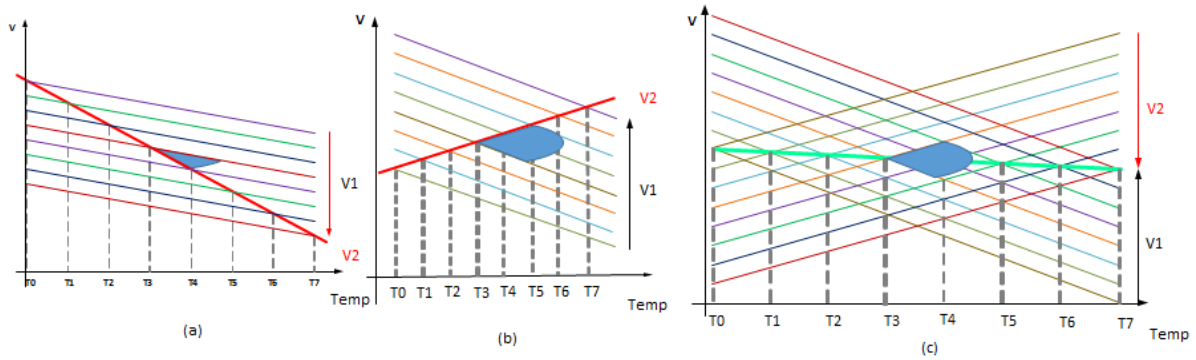


Fig. 3-17 Voltage -Temperature relationship (a) FNCN (b) FNCP (c) CNCP

For both the FNCN and the FNCP sensors, a large common-mode input range for the comparator is required to cover the entire temperature range. The common-mode input range is reduced for the FNCP sensor as shown in Fig. 3-17(c) since the locus of the intersection points as emphasized by the green line in Fig. 3-17(c) is nearly horizontal. The common-mode input requirements and offset voltage requirements of the three different sensor types are summarized in Table 3-1.

Table 3-1 Comparison of comparator offset and common-mode signal swing for three different types of TDCs

	Offset Requirements	**Common-Mode Signal Swing**
FNCN	large	Large
FNCP	small	Large
CNCP	small	Small

3.2.1. Improved TDC structures

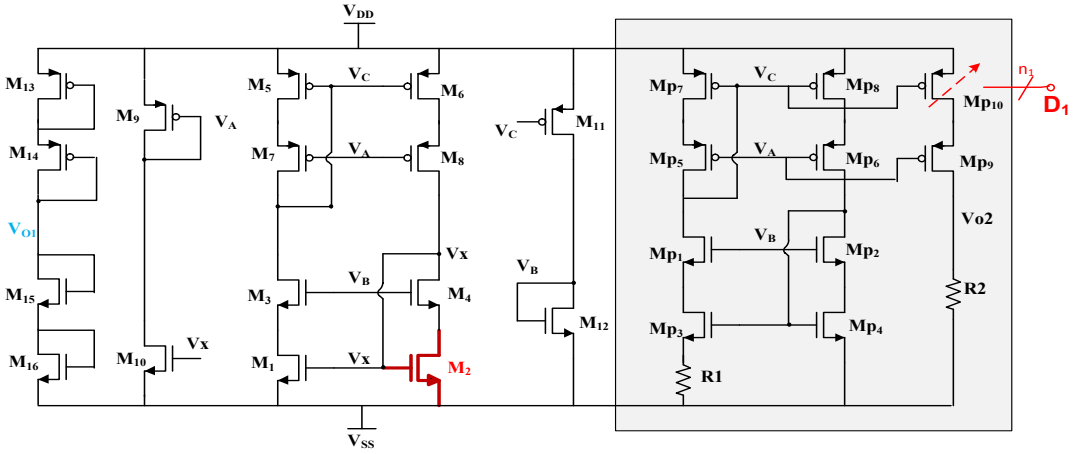


Fig. 3-18 FNCP type Temperature Sensor Core for FNCP TDC

Examples of CMOS PTC and NTC temperature sensors were introduced in CHAPTER 2. In this section they will be combined to form FNCP and/or CNCP sensors. In addition to reducing the offset voltage requirements in the comparator and limiting the common-mode input range of the comparator, the FNCP and the CNCP based TDCs are not vulnerable to the statistical separation of the two threshold voltage terms discussed in Sec. 3.1.4.

A FNCP structure is shown in Fig. 3-18 where V_{01} is the NTC voltage and V_{O2} is the PTC voltage. The PTC generator shown in the grey shaded box is a cascoded variant of the PTC generator of Fig. 2-2 and the NTC generator is a cascoded version of the NTC core of Fig. 3-4. The voltages Vo1 and Vo2 can be modeled by the equations

$$\begin{aligned} V_{O1} &= \alpha_1 + \beta_1 \mathrm{T} \\ V_{O2} &= \alpha_2 + \beta_2 \mathrm{T} \end{aligned} \tag{3.17}$$

where α_1 and α_2 are the 0K axis intercepts of Vo1 and Vo2 and where $\beta_1$and β_2 are the temperature coefficients of V_{o1} and V_{o2} respectively. The temperature coefficients satisfy the inequalities $\beta_1<0$ and $\beta_2>0$. The parameters α_2 and β_2 are dependent upon the gain of the Mp7:Mp10 current mirror which is set by the n=bit Boolean input to the PTC core.

A TDC based upon the FNCP circuit is shown in Fig. 3-19. At the differential input of comparator, the voltage is ΔV that is proportional to the temperature.

$$\Delta V_O = V_{O2} - V_{O1} = (\alpha_2 - \alpha_1) + (\beta_2 - \beta_1)\mathrm{T} \tag{3.18}$$

The logic block in the feedback loop of the TDC will reconfigure the temperature sensor in such a way that the input temperature is encoded in the digital output code D when V_{O1} equals to V_{O2}. This can be represented by the equations

$$\Delta V_O = V_{O2} - V_{O1} = (\alpha_2(D) - \alpha_1) + (\beta_2(D) - \beta_1)\mathrm{T}=0 \tag{3.19}$$

Or equivalently by the explicit expression

$$T = \frac{\alpha_1 - \alpha_2(D)}{\beta_2(D) - \beta_1} \tag{3.20}$$

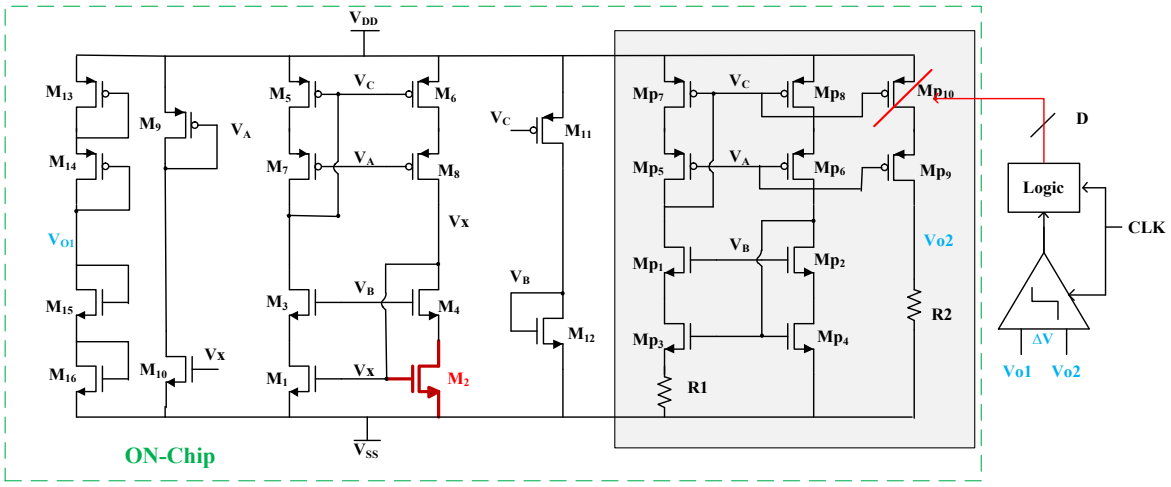


Fig. 3-19 New proposed FNCP type TDC

Correspondingly a CNPC type temperature sensor is shown in Fig. 3-20. Details of this structure will not be developed in this thesis beyond the observation that when incorporated into a TDC the temperature expression corresponding to (3.21) can be expressed in terms of the two Boolean signals D_1 and D_2 by the equation

$$T = \frac{\alpha_1(D_2) - \alpha_2(D_1)}{\beta_2(D_1) - \beta_1(D_2)} \tag{3.21}$$

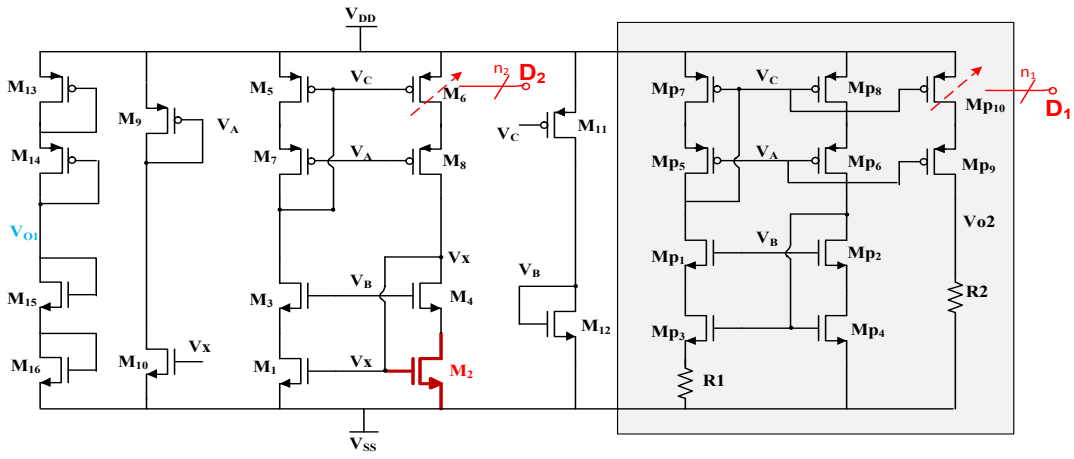


Fig. 3-20 CNPC type Temperature Sensor core for CNPC TDC

3.2.2. Simulation results for FNCP TDC

Although V_{o1} is dependent dominantly on threshold voltage and is nearly linearly dependent upon T, the temperature coefficient and V_{o2} depends on not only the threshold voltage but also on electron mobility and the temperature dependence of the mobility is somewhat nonlinear. Though the nonlinearity of V_{02} may result in a modestly nonlinear relationship between Boolean code and T, this nonlinearity can be cancelled out in the digital domain. In this section simulation results for the FNCP TDC of Fig. 3-18 implemented in IBM 0.13um process will be discussed. The comparator was dynamic latch structure but aside from the offset voltage and common-mode input range, the characteristics of the comparator are not critical to the operation of the TDC.

Device dimensions for an implementation of the FNCP TDC are given in Table 3-2. This TDC was designed for operation with a supply voltage of 1.2V in a 0.13μm CMOS process. The architecture of the 8-bit programmable current mirror M_{p10} is shown in Fig. 3-21.

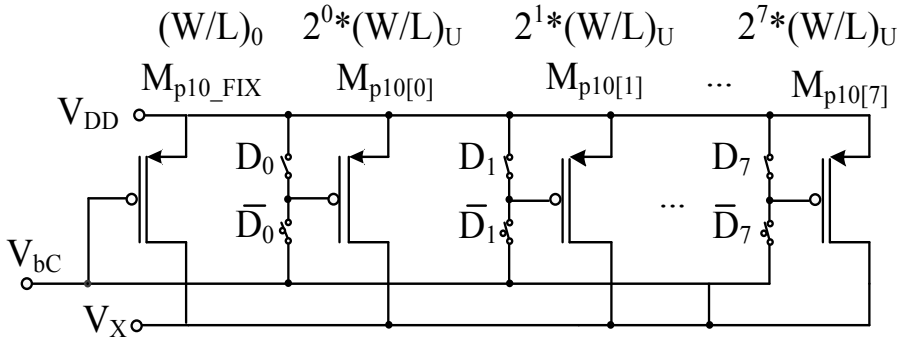


Fig. 3-21 Programmable Current Mirror Structure

Table 3-2 Implementation Details of FNCP TDC

PTC			
Device	size	Device	size
Mp5,Mp6, Mp7, Mp8	64(32u/1.2u)	Mp9	96(32u/1.2u)
Mp1, Mp3	32(32u/1.2u)	Mp10	64(32u/1.2u)
Mp2, Mp4	8(32u/1.2u)	Mp10[7:0] unit	(2.25u/1.2u)
R1	2.25k	R2	11.25k
NTC			
Device	size	Device	size
M_1	2×(3.8μ/2μ)	M_{10}	0.3u/1u
M_2	0.3μ/1μ	M_{11}	4(3u/1u)
M_3, M_4,	8×(3μ/1μ)	M_{12}	0.3/1.8u
M_5,M_6,	4×(3μ/1μ)	M_{13}	4×(3μ/1μ)
M_7, M_8	8×(3μ/1μ)	M_{14}	8×(3μ/1μ)
M_9	3.4u/1	M_{15}	(0.3μ /0.6μ)

The performance of the TDC is not strongly dependent upon matching requirements beyond those that affect the offset voltage of the comparator. However, process parameter variations do affect the performance of the TDC. In this section simulation results will focus on the statistical variation of the process parameters but not on the effects of local random variations however the Monte Carlo simulations included both the dominant process variations and the local random variations as variables. The Monte Carlo simulations were run using the Spectre simulator in the Cadence toolset.

Monte Carlo simulation results for process variations of the 8-bit digital code versus temperature are shown in Fig. 3-22 for 40 runs. It can be observed that the results all show a similar trend, that is, a well-behaved transfer characteristic with a smooth nonlinearity that can be removed digitally with calibration.

The entire set of Monte Carlo outputs was treated as a "batch" and with this definition of a batch, batch slope and batch calibration was done with a one-point temperature calibration. The results of a slope and batch calibration along with the one point level shift calibration are given in Fig. 3-23. The nonlinear error over the 100°/C temperature range is +4°C to -8°C. The nonlinearity is due primarily to the nonlinearity of the mobility with temperature and due to the channel length modulation. But since the curvature effects are similar, a batch curvature calibration can be done in the digital domain to improve the results. The simulated results with batch curvature compensation are shown in Fig. 3-24. These results show the temperature error is less than ±2°C over a 100°C operating range. One of the target applications of the TDC is power/thermal management. In these applications, the operating range over which accurate temperature measurements are required is much narrower, often 20°C or less. If the temperature range is reduced to 20°C and the calibration point is near the middle of that operating range, the temperature error will be less than ±1°C which is better than what most published results suggest is required for such temperature sensors.

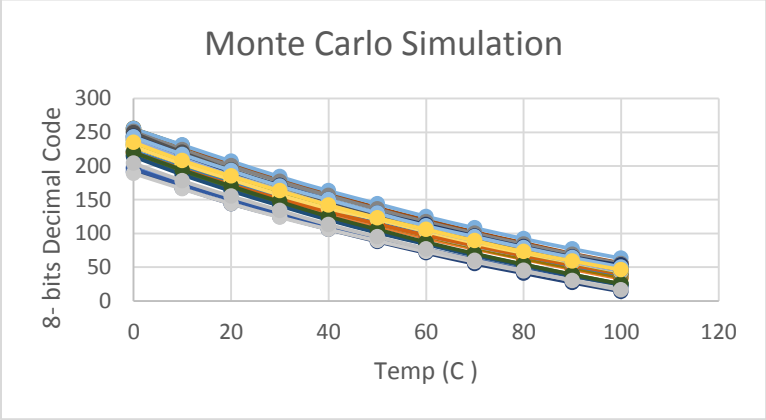


Fig. 3-22 Monte Carlo simulation of the digital output without calibration

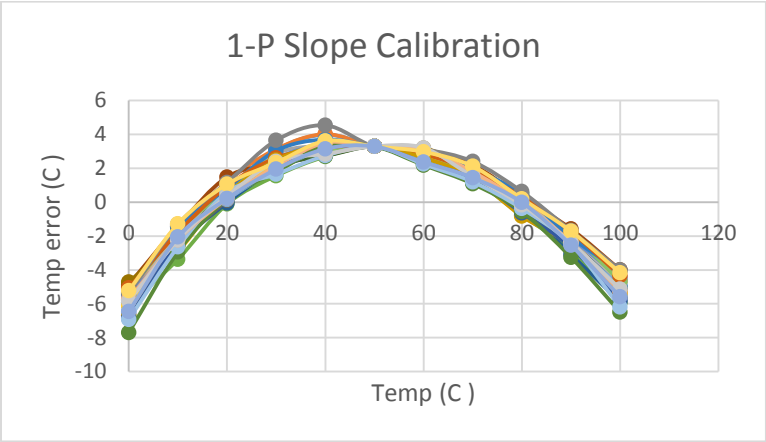


Fig. 3-23 Monte Carlo simulation of the digital output with one-point/slope calibration

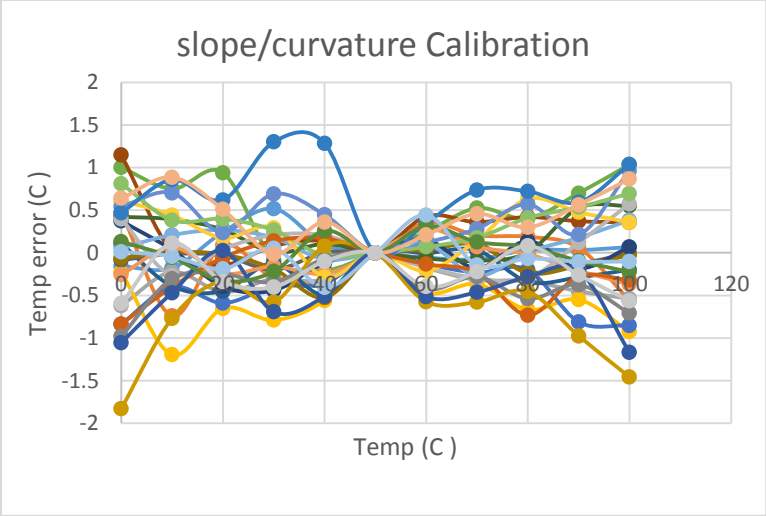


Fig. 3-24 Monte Carlo simulation of the digital output with one-point/slope/curvature calibration

The batch calibration method used for this Monte Carlo analysis used the entire population that included all process variations as the batch. A much more common approach is to do batch calibration at the wafer lot level or occasionally at the wafer level. At the wafer lot level, the statistical variations of the process parameters are dramatically smaller. We did not have good statistical models available for either the lot-level variations or the wafer-level variations in a lot so cannot predict performance with lot level or wafer-level batch slope and curvature compensation but the anticipated performance is much better than what is shown in Fig. 3-24.

3.3. Measurement Results

The fully-cascoded TDC of Fig. 3-9 has been designed in a 0.13μm process with a 1.2V power supply to support power management applications. The schematic of the comparator is shown in Fig. 3-7. The device sizes for all transistors are listed in Table 3-3.

Table 3-3 Design detail for fully-cascode TDC

Temperature sensor core			
Device	size	Device	size
M_1	2×(3.8μ/2μ)	M_{14}, M_{17}	8×(3μ/1μ)
M_2	0.3μ/1μ	M_{15}, M_{18}	(0.3μ /0.6μ)
M_3, M_4,	8×(3μ/1μ)	M_{16}	(0.41u/1u)
M_5,M_6,	4×(3μ/1μ)	M_{19}	3u/0.6u
M_7, M_8	4×(3μ/1μ)	M_{20}	3u/0.6u
M_9	3.4u/1	M_{14}[0]	(0.32u/2.4u)
M_{10}	0.3u/1u	M_{14}[1]	1(0.32u/1.2u)
M_{11}	4(3u/1u)	M_{14}[2]	2(0.32u/1.2u)
M_{12}	0.3/1.8u	M_{14}[3]	4(0.32u/1.2u)
M_{13}	4×(3μ/1μ)		
Comparator			
Device	size	Device	size
M_{21}, M_{22}	8(2×3μ/3μ)	M_{33}, M_{34}	8×(0.5μ/1.2μ)
M_{23}	4×(2μ/1.2μ)	M_{35}, M_{36}	4×(0.5μ/1.2μ)
M_{24}	4×(1μ/1.2μ)	M_{37}, M_{38}	4×(0.5μ/1.2μ)
M_{25}, M_{26}, M_{27}, M_{28}	4×(0.5μ/3μ)	M_{39}	1.2μ/0.2μ
M_{29}, M_{30}, M_{31}, M_{32}	0.4μ/0.2μ	M_{40}	0.4μ/0.2μ

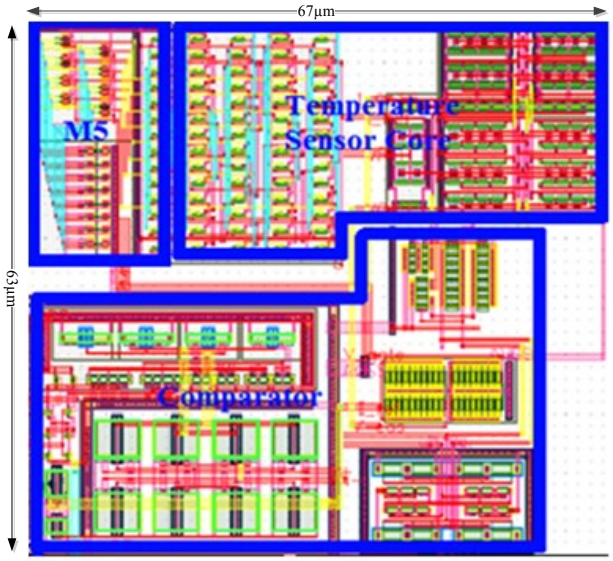


Fig. 3-25 TDC layout

The layout of the TDC is shown in Fig. 3-25. The TDC area exclusive of bonding pads and the SAR logic is 63×67 µm^2 and the target operating range is [60 °C., 90 °C.]. 4-bits of resolution were used for the programmable transistor M_{14} to demonstrate the basic operation of the TDC; nevertheless, the resolution can be readily increased if more resolution is needed with minimal impact on either area or power dissipation. The inherent linearity of digital output will not be affected by the resolution of M_{14}.

The measurement results are quantization noise free because during testing D_{OUT} was set to a certain code and the temperature was swept to find the actual temperature at which the transition of the comparator occurred. Thermal testing was done in a Fluke 7103 microbath using 3M FluC-40 monitored with F200 controller and T100-250-18 Probe

The relationship between digital code and temperature is shown in Fig. 3-26. The comparator offset was set to make V_1-V_2=0 at 60 °C when the D_{OUT} code is 1111. This provides for full range use of the four digital codes.

The temperature error for 5 samples is shown in Fig. 3-27 with one point batch slope calibration at code 0111. The results show the error is bounded by ±0.3°C. It can be observed that all show about the same curvature. If batch curvature correction is added, the error would be much less.

Two-point calibration and batch curvature compensation was also done. The results are shown in Fig. 3-28. With the two-point calibration the temperature error reduces to ±0.1 °C. For most on-chip power management applications, publications coming from several semiconductor companies suggest ±3°C accuracy is good enough though some research in our group suggest that ±0.5°C accuracy over a ± 15°C range is needed to achieve reasonable reliability metrics when power/thermal management is used to manage thermal/electrical wear. Regardless, this TDC with single-point calibration should provide performance at a level that is needed for the target power/thermal management application.

Table 3-4 shows the comparison between several smart temperature sensor designs. It is somewhat difficult to make comparisons when the sampling rates and feature sizes differ so much and when temperature ranges vary so much as well. Two metrics are included in this table that partially correct for the differences in feature sizes and sampling rates. The normalized area (Area Norm) is the ratio of the die area to the square of the feature size (in $mm^2/\mu m^2$). The normalized power (Power Norm) is the product of the power dissipation and the sampling period (in mWμsec). When focusing on the power management application, the proposed work shows good accuracy with a single point calibration with extremely low area and low power dissipation. The normalized area and the normalized power performance of the proposed TDC are much better than that of the popular comparative structures.

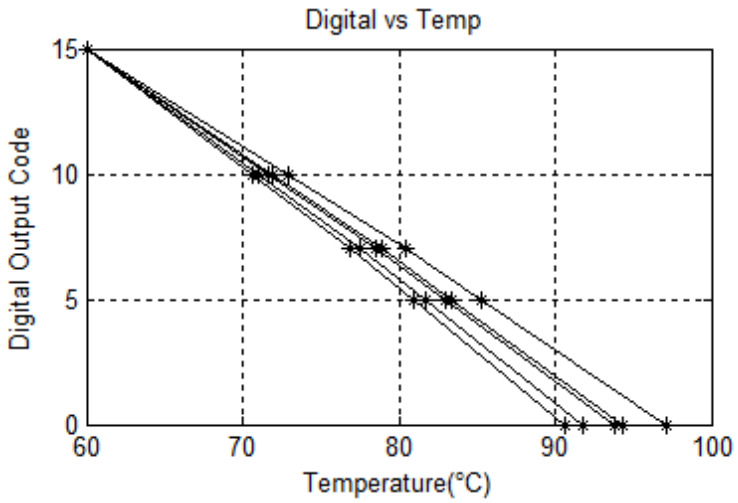


Fig. 3-26 Digital code vs. Temperature

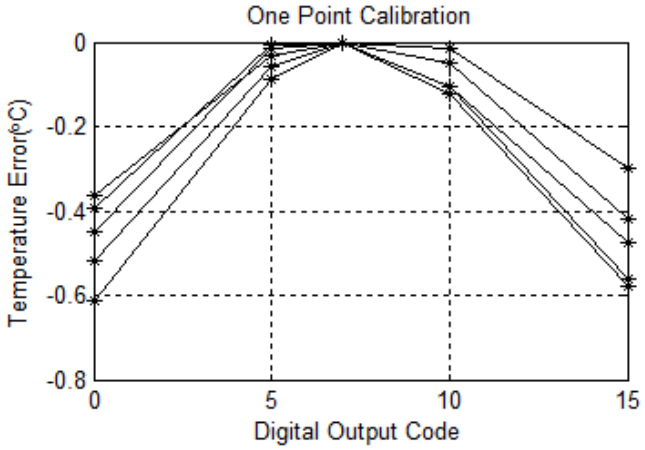


Fig. 3-27 Temperature error with one point batch slope calibration

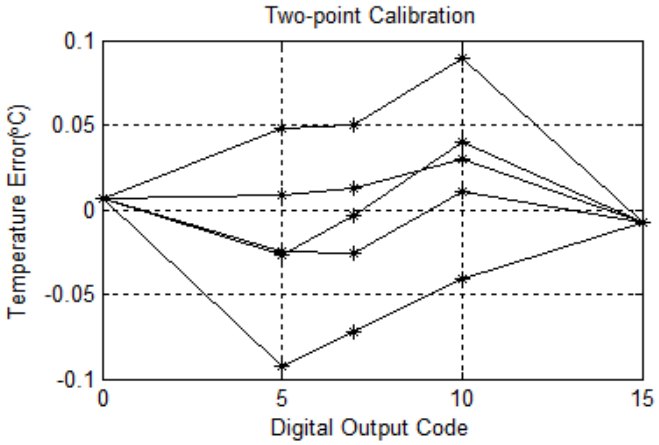


Fig. 3-28 Temperature error with two point batch curvature calibration

Table 3-4 Comparison of the digital temperature sensor

Temp Sensor	This work	Law [12]	Chen [8]	Pertijs [4]	Shors [3]	
Feature Size (μm)	0.13	0.18	0.35	0.7	0.032	0.022
Error (°C) (1-point)	-0.6			±0.1	±4.5	
Error (°C) (2-point)	±0.1	±0.9	±0.8			±1.5
Power (mW)	0.0816	1.19E-4	0.01	0.421	3.78	1.4
Sampling Period (uSec)	1	3000	5E5	1E5	10 to 100	
Area (mm^2)	0.0025	0.042	0.175	4.5	0.02	0.0061
Temp Range (°C)	60~90	-10~30	0~100	-55~125	-10~100	
Area Norm ($mm^2/\mu m^2$)	0.15	1.30	1.43	9.18	19.53	12.60
Power Norm (power*period)	0.0816	0.357	5000	42100	37.8~ 378	14~ 140

CHAPTER 4 VERIFICATION

Throughout much of the analog and digital VLSI communities, verification focuses primarily on determining whether a circuit that has been designed will meet desired system requirements. Invariably it is assumed there is a unique and predictable output for any set of inputs. In the context of this thesis, the concept of verification is much different. Specifically, in this work, verification refers to the task of determining whether a nonlinear circuit has an undesired or unintended mode (or modes) of operation in addition to the desired mode of operation. That is, can a circuit operate under normal input conditions as desired but under some other input conditions can the same circuit operate in a different and undesired mode?

Self-stabilized bias generators, voltage and current references, log-domain filters, and bootstrapped feedback networks are well-known applications where undesired stable operating modes can occur [16-19,33,34]. But there are many other applications where Trojan operating modes can occur as well. Designers are aware of this vulnerability in many of these circuits and invariably add circuits termed “startup” circuits to remove the undesired mode of operation.

Prior to this work, concerns existed about whether a circuit had undesired equilibrium points or undesired dynamic modes of operation that occurred through oversight of trusted engineers and that could escape detection using conventional simulation and verification tools. These concerns were addressed primarily by relying on the experience of designers to identify potential problem and identification methods were primarily viewed as an art. Early in this work, my focus on this problem was primarily on understanding the basic principles behind this undesired operating mode problem and on establishing strategies to

systematically identify vulnerabilities that could be incorporated into a verification methodology. But as this work progressed, it became apparent that these undesired modes of operation that were occasionally and unintentionally introduced by talented, experienced, and trusted engineers had many properties of a hardware Trojan that could be maliciously inserted into a circuit. And with no known methods for determining if a circuit can exhibit such an undesired mode of operation even with the best available simulation and verification tools, it became apparent that the industry has a major vulnerability that can be exploited if these modes of operation are intentionally inserted by an adversary and that are intentionally inserted in such a way that detection of their presence is extremely difficult. Because of these vulnerabilities and because these undesired modes of operation can have properties that are typical of hardware Trojans, the undesired modes of operation will be interchangeably be denoted as Trojan states or Trojan modes throughout the remainder of this thesis. And the circuits that are used to remove or eliminate the Trojan states or Trojan equilibrium points will be termed Trojan State Elimination (TSE) circuits.

Although the presence of Trojan operating points are often known early in the design process, on occasion designers are not aware of the presence of Trojan operating points until after circuits have been fabricated. The task of identifying the presence of Trojan operating states and verifying removal with startup circuits is complicated by the fact that existing circuit simulators provide a single solution (or operating point), not multiple operating points nor all operating points when more than one operating point is present.

TSE techniques have been studied and developed for different applications but the widespread use of term “startup” circuits for the circuits that are intended to mitigate the undesired operating point problem can be misleading since startup is often associated with a

temporal process of controlling when biasing voltages actually appear in different parts of a system when power is supplied to a circuit. Using a "startup" circuit to control the circuit when power is applied may circumvent having the circuit enters an undesired stable state most of the time but if the stable Trojan state exists, unanticipated transients can cause the circuit to enter the Trojan state and thereby cause the circuit to fail. It may also contribute to the widespread but ineffective use of slow supply ramps to assess whether a TSE circuit is effective. Regardless, the need for a TSE circuit is often not apparent and often recognized only by the experience of a circuit designer.

Several methods have been developed for finding multiple operating points in a circuit when it is conjectured or known that more than one operating point exists [35,36]. Some algorithms based upon piecewise-linear approximations of all nonlinear devices provide all operating points of a circuit [37,38] but implementation of these algorithms for even simple circuits is tedious and computation time is prohibitive if the circuit is very large. Homotopy methods are widely used to trace DC solutions though these methods do not guarantee all operating points will be identified and computation time can be large as well. Some papers also discuss how to determine whether an operating point is stable or unstable after the operating point has been identified [39,40]. However, simple and efficient methods that are guaranteed to find all operating points in either SPICE or SPECTRE in even rather simple circuits do not exist.

In this dissertation, simple methods for verifying the effectiveness of TSE circuits for removal of known Trojan states will be discussed. Two examples will be given to demonstrate the issues. Though the methods are applicable to a large number of well-known circuits that are vulnerable to the existence of Trojan states, emphasis here will be restricted

to applying these methods to a threshold-voltage-based temperature sensor and a Bandgap reference.

4.1. Start-up Issue and Traditional Verification Method

Simulation of a circuit to verify whether a startup circuit is needed or whether a startup circuit is robust can be challenging. Designers usually assume that a startup circuit is not needed if simulations of the reference circuit, either static or transient, do not show the existence of a second stable operating point. If simulations do not show the existence of a second stable operating point, it is often concluded that the reference circuit always works appropriately. If any simulation of the reference circuit shows the existence of an undesired stable operating point, it is tempting for the designer to add a startup circuit and observe that the undesired stable operating point disappeared when the simulation is repeated. But, since any simulator will only provide one solution to a circuit, there is no assurance that if simulations of the reference do not present an undesired stable operating point that such a point does not exist. Actually, the designer may be really unlucky if simulations of a circuit with two stable equilibrium points always result in the desired stable operating point as these simulations would mask the presence of the undesirable stable operating point.

A standard practice in industry for verifying that a TSE circuit is effective is to run repeated transient simulations, often with a linear ramp up of the supply voltage, to verify that the circuit "starts up" correctly. With this approach, an incorrect startup would occur if the circuit entered an undesired stable equilibrium point. If an incorrect startup is not observed, the designer concludes that the circuit does not have a startup problem. With this approach, it can only be concluded that if all energy storage elements in the real circuit have the same initial conditions as were used in the simulation and if the supply voltage ramp

agrees with the simulation ramp, then the circuit will reach the observed operating point after an acceptable delay from the time the transient analysis starts. Although this approach often results in TSE circuits that serve the intended purpose, it does not guarantee that all serve the intended purpose and most importantly it does not guarantee that all undesired stable equilibrium points have been eliminated. If all undesired stable equilibrium points have not been eliminated, an unanticipated sequence of transient events during normal operation can cause the circuit to move to an undesired stable equilibrium point. And even if the undesired stable equilibrium points have been eliminated for the conditions specified in the transient simulation, process and temperature variations may cause an undesired stable equilibrium point to reappear.

4.2. Circuit-level Homotopy Method

Circuit-level continuation methods for TSE verification often involve the introduction of a voltage or current source that can be swept to trace operating points of a circuit. This can be viewed as a homotopy approach implemented at the circuit level. The terms "continuation methods" and "homotopy" approaches will be used interchangeably in the remainder of this thesis. When certain conditions are satisfied, homotopy approaches can be used to identify valid operating points of a circuit. The most common approach in this class involves insertion of sources that do not break any loops in the circuit thereby circumventing concerns about loop loading when a feedback loop is broken. Methods in which feedback loops are broken can also be used provided the operating points are not disturbed by breaking the loops. Much like the challenges faced by designers of feedback systems that rely on simulation of the open loop transfer characteristics, or what is often simply termed the loop

gain, it is critical that breaking the loop with homotopy methods does not alter the basic operation of the circuit at any actual operating point.

4.3. Intact-Loop Continuation Methods

Green [41] proposed an intact-loop continuation method to verify the effectiveness of a startup circuit in removing a known Trojan operating point. With the Green method, a voltage source is inserted between two nodes in the circuit and the voltage is swept over a predetermined range and the current flowing through the voltage source is monitored. All points on the resultant voltage-current transfer curve where the current is 0 are operating points of the circuit and these operating points could be stable or unstable points. This method is simple and computationally efficient and for many useful circuits, the operating points this method identifies are all operating points of the circuit. Fig.4-1(a) shows application of the Green method to the inverse-Widlar bias generator. But, in general, it cannot be guaranteed that this method will identify all operating points.

A counterpart intact-loop continuation method involves inserting a current source in a branch of the circuit as shown in Fig. 4-1(b). With this method, sweeping the current will provide operating points of the original circuit at all points where the voltage across the current source equals zero. This method is also simple and computationally efficient and for many useful circuits will identify all operating points. However, with the latter method, determination of the range over which the current should be swept may require some effort. And, like the Green method, it cannot be guaranteed that this method will identify all operating points in all circuits.

Both methods suffer from the requirement of very accurately simulating the circuit at very low currents since two of the operating points of the inverse-Widlar circuit are obtained when one or more devices in the circuit are operating in deep weak inversion. With the current-sweeping of Fig. 4-1(b), it can be shown that it suffices to consider only positive currents and thus a logarithmic sweep can be useful for identifying low-current operating points. The corresponding use of a logarithmic voltage scale for voltage scanning is not useful for identifying where currents vanish with the Green method.

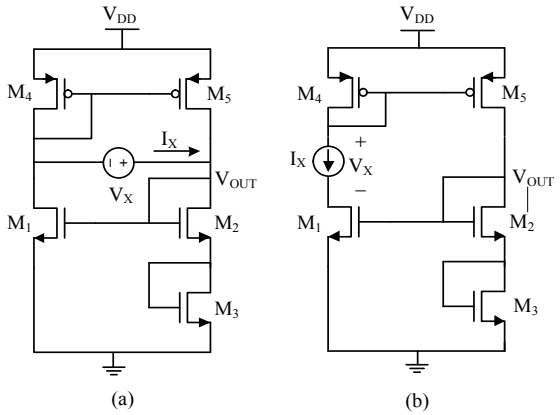


Fig. 4-1 Intact continuation method (a) voltage node sweeping type (b) current branch sweeping type

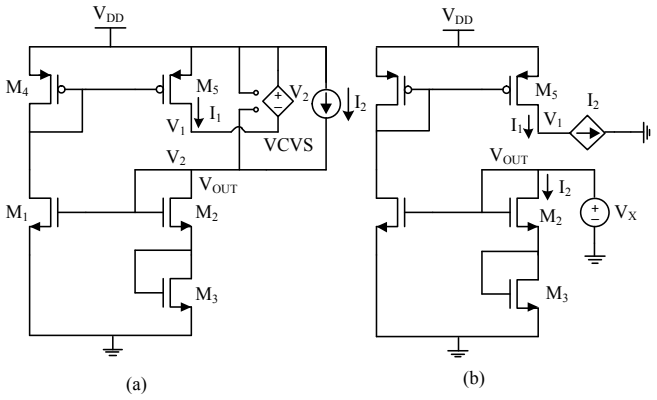


Fig. 4-2 Break-loop continuation method (a) current branch sweeping type (b) voltage node sweeping type

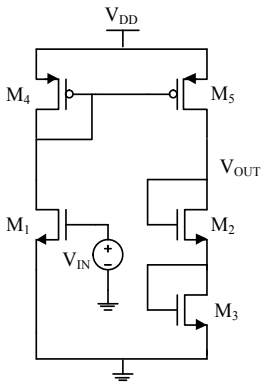


Fig. 4-3 A special case for break-loop voltage node sweeping

4.4. Break-loop Continuation Methods

A continuation method that involves breaking the feedback loop [42] and driving the loop with a current source at the break is shown in Fig 4-2(a). With this approach, a voltage controlled voltage source (VCVS) is incorporated to assure that loop loading is not altered at the operating points of the circuit and a sweep is made of the current I_2. Any branch voltage that is generated by the VCVS from the sweep when $I_1=I_2$ is an operating point. Since it can be shown that the current I_1 in this circuit is always positive, a logarithmic current sweep is useful for identifying the operating points of this circuit when the devices operate in weak inversion. Another continuation method that involves breaking the feedback loop and driving the loop with a voltage source at the break node is depicted in Fig 4-2(b). With this approach, a current controlled current source (CCCS) is incorporated to assure that loop loading is not altered at the operating points of the circuit and a sweep is made of the voltage V_X over a predetermined range. Any nodal voltage that is generated from the sweep when $V_1=V_X$ is an operating point. From a practical viewpoint, the sweep range can be readily determined and the need for a logarithmic sweep can be eliminated.

A third break-loop continuation method is shown in Fig. 4-3 whereby the loop is broken at the gate of a MOSFET [43] and the loop is driven by a voltage source inserted at the break, V_{IN}. Since the break is made at the gate of a MOS device where the input impedance is ideally infinite, loop loading is not affected by this break. This is applicable for MOS circuits because the input impedance of the corresponding resistive circuit[2] at the break is ideally infinite. With a readily predeter mined sweep range, any voltage where $V_{OUT}=V_{IN}$ is an operating point. This could be viewed as a special case of the approach of Fig. 4-2(b) where the CCCS is not needed since the controlling current is zero.

An implementation of the inverse-Widlar circuit has been designed for demonstrating the five methods discussed in the previous sections for finding multiple operating points. The circuit has been designed to have three operating points when operating without a TSE circuit. Two of these operating points are stable operating points and one is an unstable operating point. The device sizes for this implementation are listed in Table 4-1. All simulations were made using the Typical/Typical 1P6M 0.18um BSIM3v3 models in the Spectre simulator running under a Cadence environment. All five Homotopy methods can be used to investigate whether a circuit has multiple operating points and all do identify all operating points in many useful circuits. And all are useful for verifying the effectiveness of TSE circuits in many useful circuits as well. But all share the limitation that they cannot be used to guarantee all operating points have been identified irrespective of whether a TSC

[2] the "resistive circuit" is that part of a circuit that remains if all energy storage elements in the circuit are removed

circuit is present or absent. Simulation results demonstrating that the five homotopy methods are all capable of identifying the two stable operating points of this implementation of the inverse-Widlar circuit as well as a comparison of the methods follow.

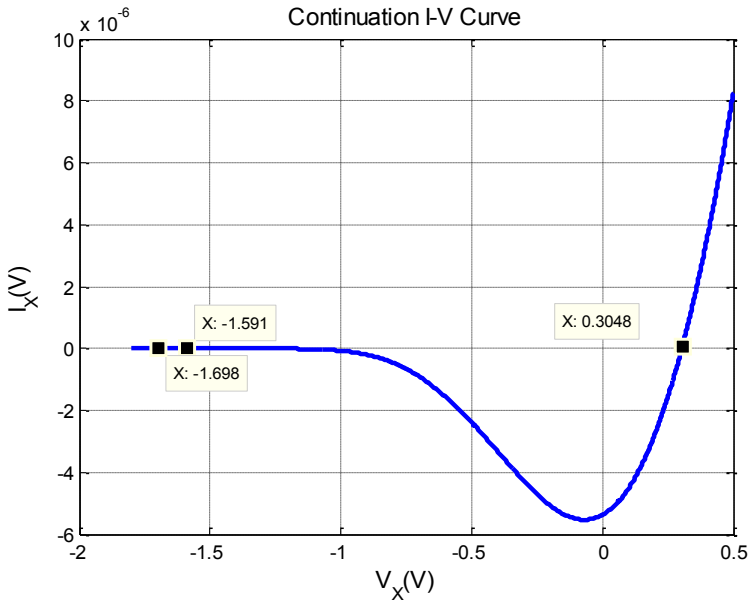
Table 4-1 Design parameter in TSMC 0.18um process

M1	M2	M3	M4	M5
0.3u/0.9u	15u/0.3u	5u/0.3u	2.4u/0.3u	2.4u/0.3u

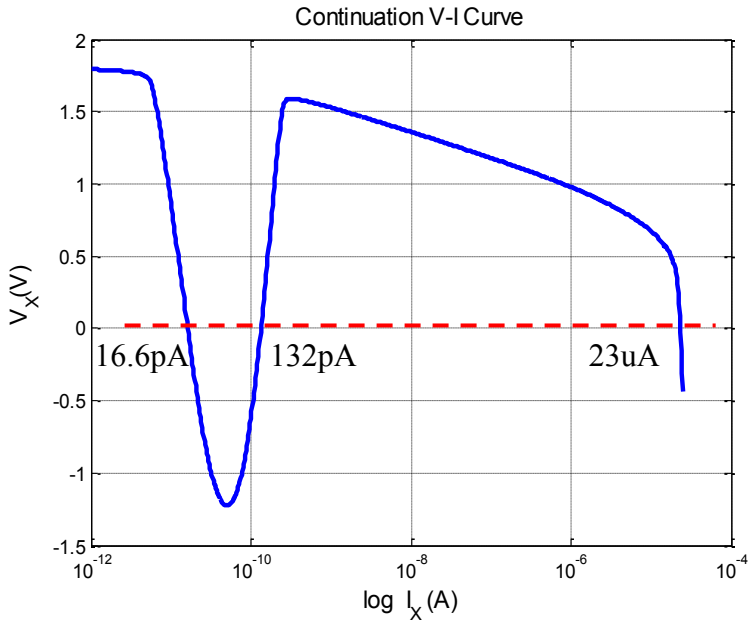
Use of the intact loop method of Fig. 4-1(a) is shown in Fig. 4-4(a). In this figure the relevant portion of the sweep of the voltage V_X results in three intersection points of the current I_X with the I_X=0 line. These occurred at V_X=-1.698, V_X=-1.591 and V_X=0.3048. The right zero crossing point at V_X=0.3048 can be observed easily but the other two operating points are not as easy to verify in the plot since they occur at very low current levels. If desired, the corresponding nodal voltages at these intersection points can be obtained. The corresponding output voltages, V_{OUT}, are 0.012V, 0.192V and 1.16V. The outputs at 0.012V and 1.16V are stable equilibrium points and the output at 0.192V is an unstable equilibrium point. The stable output V_{OUT}= 1.16 is the desired output for this circuit. The other stable output, V_{OUT}= 0.012 is an undesired output which I will refer to as the Trojan output state of this circuit. Use of the intact loop method of Fig. 4-1(b) is shown in Fig. 4-4(b). When applying a linear current source sweep of the branch current, two of the operating points will be missed unless the step size is extremely small since these two operating points occur at very low current levels. However, by using logarithmic-spaced sweep points, all three operating points are readily identified as is apparent from the intersection of the sweep with the V_X=0V line in Fig. 4-4(b). Logarithmic current sweeping is practical in this case since the current will always flow from V_{DD} to V_{SS} in the left part of the circuit. The

corresponding output voltages, V_{OUT}, at the 3 intersection points where V_X=0V are 16.6pA, 132pA and 23uA. As expected, they are the same output voltages as was obtained with the earlier intact loop method.

As expected, simulation results show that all five continuation methods successfully identified all operating points in this circuit. Fig. 4-4 shows the intact-loop continuation methods using voltage source and current source respectively sweeping respectively. In Fig. 4-4(a), with a sweep of the voltage in the circuit of Fig. 4-1(a), the right zero crossing point can be observed easily but the other two operating points are not easy to verify in the plot since they occur at very low current levels. When applying a linear current source sweep of the branch current in the circuit of Fig. 4-1(b), two of the operating points will be missed unless the step size is extremely small since these two operating points occur at very low current levels. However, with using logarithmic-spaced points, all three operating points are readily identified as shown in Fig. 4-4(b). Logarithmic current sweeping is practical in this case since the current will always flow from V_{DD} to V_{SS} in the left part of the circuit.



(a)



(b)

Fig. 4-4 Simulation results for intact-loop continuation method

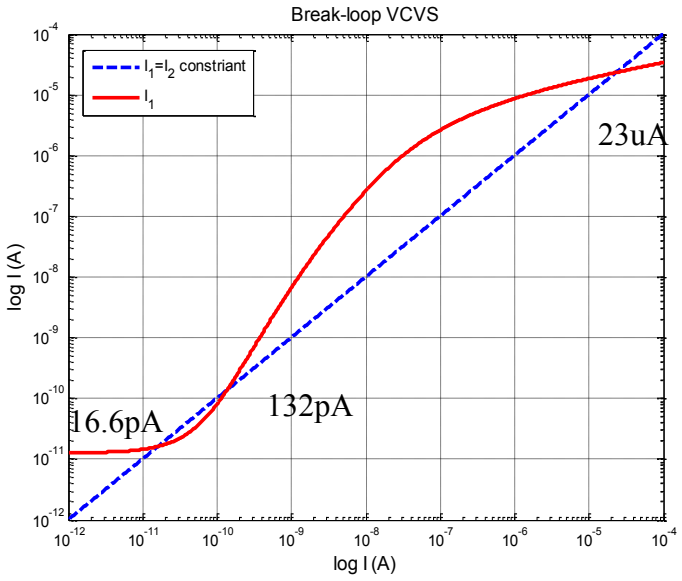
(a) Green voltage node sweeping (b) current branch sweeping type

Simulation results for the three different break-loop continuation methods are shown in Fig. 4-5. The current-current plot of Fig. 4-5(a) is based upon the current sweep of Fig.4-2(a). Although only two distinct stable operating points can be easily identified from the simulation results presented [42] when a linear axis is used, all three operating points are distinctly visible using a logarithmic sweep axis. The corresponding output voltages, V_{OUT}, at the 3 intersection points that occur where $I_1=I_2$ are $V_X=0.012$, $V_X=0.192$ and $V_X=1.16$volts. As expected, they are the same output voltages as was obtained with the earlier intact loop method.

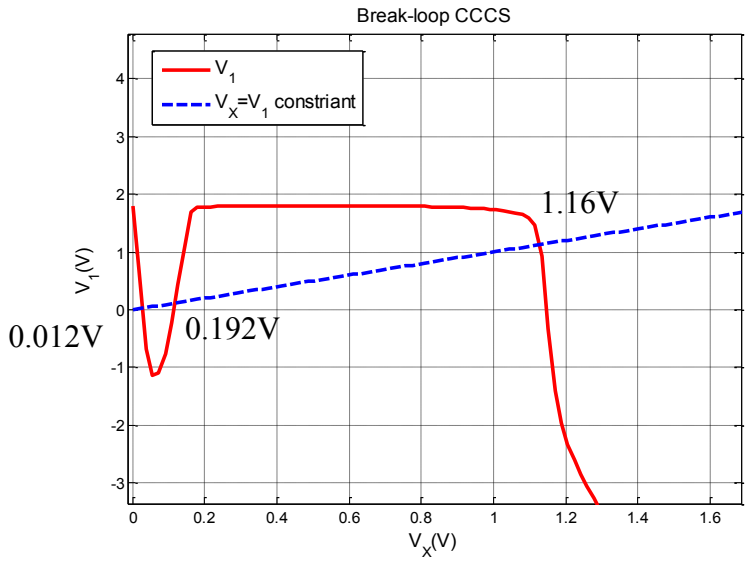
In Fig. 4-6(b), simulation results for the voltage sweep for the break-loop method of Fig. 4-2(b) are shown. All three operating points which are the intersections with the $V_1=V_X$

line are readily identified from this plot. These intersection points are at V_X=0.012, V_X=0.192 and V_X=1.16volts. Since V_{OUT}=V_X in this circuit, the output values are readily available and agree with what was obtained with the previous continuous methods.

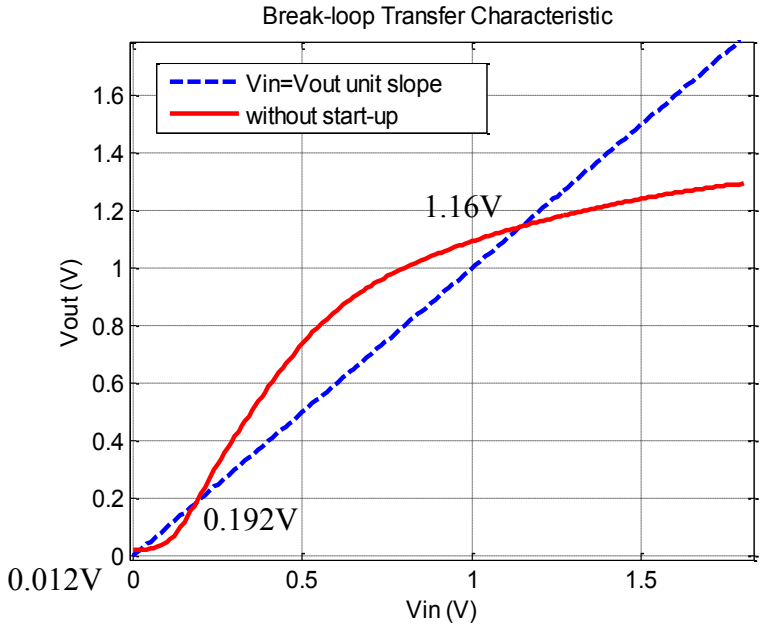
The voltage-voltage transfer characteristics from the break-loop gate voltage sweep method of Fig. 4-3 are shown in Fig. 4-5(c). In the controls community, the relation between V_{OUT} and V_{IN} in this sweep is termed the "return map". The three operating points corresponding to the intersection with the V_{OUT}=V_{IN} line are readily apparent from this plot. The corresponding output voltages, V_{OUT}, at the 3 intersection points are V_X=0.012, V_X=0.192 and V_X=1.16volts. As expected, they are the same output voltages as was obtained with the earlier continuation methods.



(a)



(b)



(c)

Fig. 4-5 Simulation results for break-loop continuation method

(a) current branch sweeping type (b) voltage node sweeping type (c) Special case

Though all five continuation methods successfully identified all operating points for this circuit, it was much easier to identify the Trojan operating state with the current sweep of

Fig. 4-1(b) and with the voltage sweeps of Fig. 4-2(b) and Fig. 4-3. When these methods are used to verify the effectiveness of a TSE circuit, simulations should be run over all process corners, over all temperatures of interest, and over supply bounds to guarantee that the Trojan operating points have been eliminated in the presence of Process, Voltage, and Temperature (PVT) variations.

A commonly used method for verifying the effectiveness of a TSE circuit, particularly in industry, is the traditional transient simulation method of slowly ramping the supply voltage. The premise is that if a TSE circuit is added, its effectiveness of eliminating undesired stable equilibrium points can be verified by slowly sweeping the supply voltage from 0 to the normal operating value. If the circuit maintains operation at the desired operating point at the end of this sweep, it is then concluded that the undesired stable equilibrium points have been eliminated with the TSE circuit.

Simulation results of a slow V_{DD} ramp for the inverse-Widlar circuit that was designed to have two stable equilibrium points and that was used to demonstrate the use of the six homotopy methods are shown in Fig. 4-6. It can be observed that the output settles to the desired operating point at 27˚C even without a TSE circuit. This example demonstrates the ineffectiveness of using this method for verifying that Trojan operating points have been removed with a TSE circuit. The same transient simulation at a higher temperature of 125 ˚C does cause this circuit to get stuck at the stable Trojan operating point though there is no guarantee that the Trojan operating point will be found by varying temperatures with this approach.

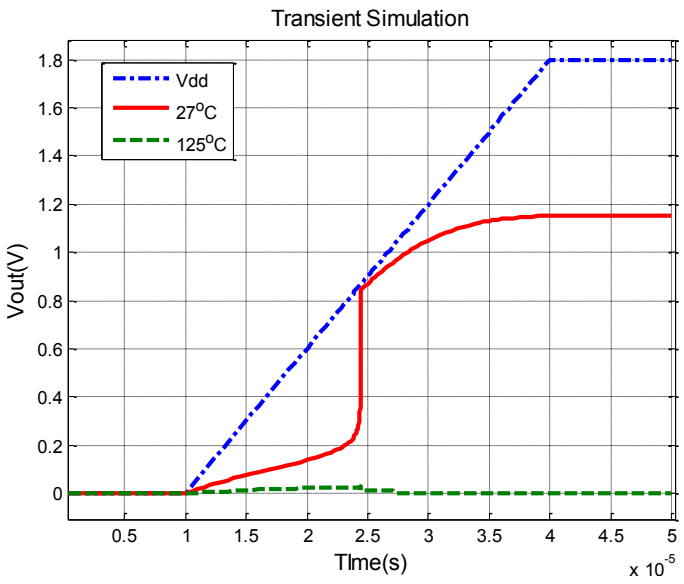


Fig. 4-6 Transient Simulation

4.5. Effectiveness of Circuit-level Continuation Methods for Trojan State Verification

From the discussions in the previous Section, one can conclude that the critical crossing points are easier to identify when the return parameter is a voltage with both the intact and break loop methods. This is attributable to the fact that for this self-bias generator, the Trojan stable operating point occurs where the transistors are working in deep weak inversion where the drain currents are extremely small.

There are two concerns about applying circuit level continuation methods to find Trojan operating points that deserve discussion. One is that the number of nodes and loops in a circuit increases as the circuit becomes more complex; therefore, the choice of which node or which loop is most useful for using continuation methods must be addressed as some work better than others. And some choices may cause these continuation methods to fail for some circuits. Even when they do work, different breaking nodes or branches result in different

transfer curves and some may provide better insight than others. Another issue is the number of steps that are needed for the sweeps since a large number of steps can result in long simulation times and since too few steps can result in failure to identify undesired equilibrium points. The sweeping range and the resolution determine the number of steps. For voltage sweeping, the range is bounded by the supply voltage for most circuits which is decisive. Determination of the current sweeping range over which the current should be swept may require more effort. Accurately simulating at very low currents is often required and this can result in requiring many steps. Regardless of how the number of steps is determined, it must be recognized that simulation time is proportional to the number of steps.

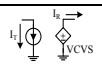
Though not the focus of the earlier discussion of the homotopy methods, it can be observed that the break-loop methods resulted in breaking of a positive feedback loop in the inverse-Widlar circuit example. It can be shown that this circuit has only one positive feedback loop and it was this positive feedback loop that was broken. That was not a coincidence but rather a key requirement for the use of the break-loop homotopy methods. In this section additional insight into how to identify and break positive feedback loops for the purpose of doing homotopy analysis will be discussed though no attempt will be made to make a complete formal characterization of either the feedback structure of a circuit or of how to identify the critical loops that must be broken when using continuation methods for determining the presence or absence of Trojan modes of operation. Considerable progress has been made on how to address these problems by both the author of this thesis and other colleagues working on these problems but as of the writing of this thesis it remains an active area of research.

We this qualification, the Trojan state verification and mitigation process will be initiated by the identification of the positive feedback loop in a circuit followed by the use of continuation methods to check the circuit for uniqueness of operating modes. If Trojan operating points are shown to exist, a TSE circuit will be added in an attempt to remove the undesired operating point. The process then will be repeated on the modified circuit to verify the effectiveness of the TSE circuit. The process can be repeated again of the initial TSE circuit proves to not successfully mitigate the Trojan state problem. Two examples will be given in this section to demonstrate the process.

4.5.1. Circuit-level continuation method

The continuation methods for finding operating points of a circuit that were discussed in the previous two sections are summarized for convenience in Table 4-2 Though not specifically noted in the table, the fifth method discussed above which is often the most useful is a special case of the Break loop Voltage Return approach.

Table 4-2 Circuit-Level Continuation Methods

	Continuation Method			
	Intact loop		***Break loop***	
	Current return	**Voltage return**	**Current return**	**Voltage return**
Test, x	V_T	I_T	I_T	V_T
Return, f(x)	I_R	V_R	I_R	V_R
Solution Condition	$I_R=0$	$V_R=0$	$I_R= I_T$	$V_R=V_T$
Symbol				

4.5.2. Loop identification

For simple circuits, feedback loops can be manually identified by the designer. But the development of practical methods that can automatically and systematically find all feedback loops in larger scale circuits is an open research problem. This is complicated by the observation that circuits can contain multiple loops and these loops may be intertwined and couple together. Nevertheless, many well-known and useful circuits that are vulnerable to the presence of multiple operating points, such as bias generators, Bandgap references, and temperature sensors, contain only a single positive feedback loop. This property will lessen the challenge for finding the operating points.

We now focus on single positive feedback loop circuits. First we convert the circuit to a weighted directed graph. There may be more than one way that this conversion can be done. Based on well-developed graph theory, the graph is comprised of nodes and weighted edges. The weight on each directed edge will be either +1 or -1. Loops can exist in the graph. The loop is termed a positive feedback loop if the number of directed edges associated with the loop has an even number of "-1" weights that is greater than or equal to 2.

A temperature sensor example based upon the inverse Widlar structure is shown in Fig. 4-7. The node-link diagram for the graph of the Inverse-Widlar structure is shown in Fig. 4-7(b). The vertices in the graph correspond directly to the non-ground nodes in the circuit so the same labels have been used. The edges correspond to the transistors that are providing amplification. This graph has a single loop $<N_1\ b_2\ N_3\ b_1>$ and since the weights of the two edges are both -1, this is a positive feedback loop. Mapping back from the positive feedback loop to the circuit schematic, the branch b_1 corresponds to transistor M_5 and the branch b_3

corresponds to the transistor M_1.M_1 and M_5 are common source amplifiers with negative gain and comprise a positive feedback loop in the circuit.

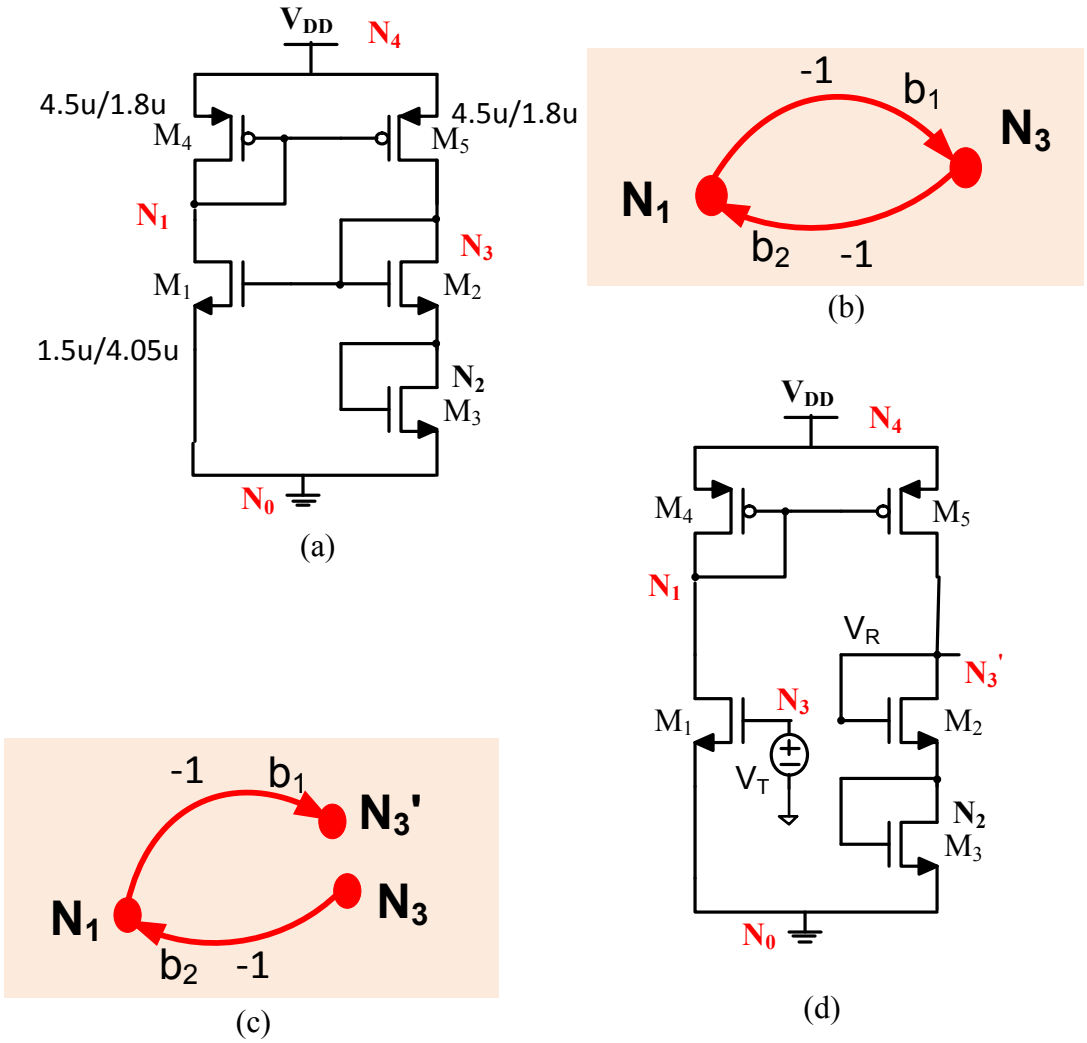


Fig. 4-7 (a) Inverse-Widlar Circuit (b) Node-Link Diagram (c) Node-Link Diagram of Vertex Break (d) Open-loop circuit for homotopy sweep

Next, a homotopy method will be applied to the positive feedback loop. Any of the homotopy methods summarized in Table 4-2 can be used. As an example, the break-loop voltage return method will be demonstrated. The positive feedback loop can be broken at any vertex in the loop. In this example, the vertex **N_3** will be selected as the break vertex.

This break vertex is mapped to two vertices, denoted as **N_3 and N_3'** . The resultant graph obtained by breaking the positive feedback loop at **N_3** is shown visually in the node-link-diagram of Fig. 4-7(c). The corresponding open-loop circuit must then be obtained by mapping from the open-loop graph back to the circuit. The circuit loop will be broken at the node **N_3** and decomposed into two nodes **N_3** and **N_3'**. The corresponding circuit that can be used for the homotopy analysis is shown in Fig. 4-7(c). For this open-loop circuit the return map is create by exciting the circuit at node **N_3** with the test voltage V_T and the resultant output voltage is that obtained at node **N_3'** and denoted as V_R.

A second example is the Banba bandgap reference[44] shown in Fig. 4-8(a). The node-link diagram for the graph of this circuit is shown in Fig. 4-8(b). This circuit has two feedback loops but only one is a positive feedback loop <**N_1 b_2 N_3 b_1**> and it is highlighted in red in the node-link diagram. This positive feedback loop can be broken 3 different ways. One is at vertex **N_1** and the other two are at vertex **N_3**. These three methods for breaking the positive feedback loop are depicted in Fig. 4-9(a). But the three different ways to break the positive feedback loop will result in different characteristics in a homotopy analysis though all should give the same results. Fig. 4-9(a) and Fig. 4-9(c) show breaks that will keep the negative feedback loop intact. The corresponding breaks in the circuit using the break-loop voltage return method will result in a monotone return map if the negative feedback loop is left intact. If the positive feedback is broken as indicated in Fig. 4-9(b), both the positive and negative feedback loops will be broken and the corresponding breaks in the circuit will result in a non-monotonic return map because the negative feedback mechanism will also be disabled. Though the issue of monotonicity of the return map does not affect the ability to identify the equilibrium points, strategies for significantly reducing the simulation time have

been developed by others working on this project in our research group that are applicable if the return map is monotone.

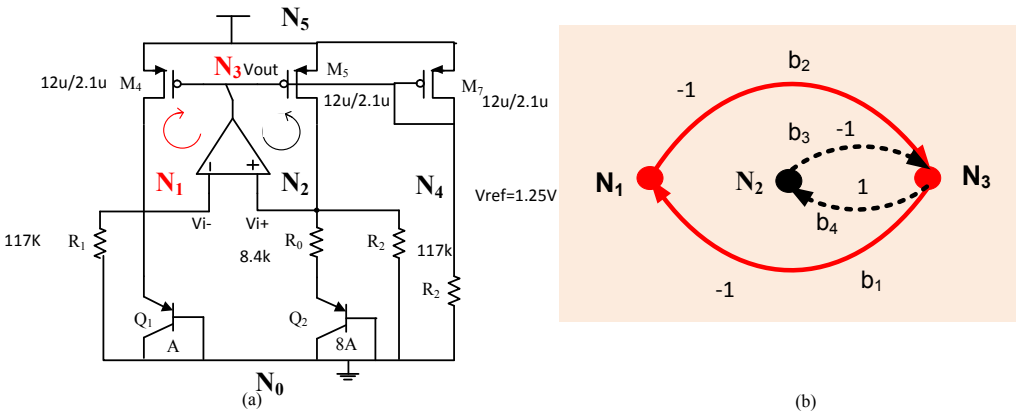


Fig. 4-8 (a) Banba Bandgap reference (b) Node-link diagram for circuit graph

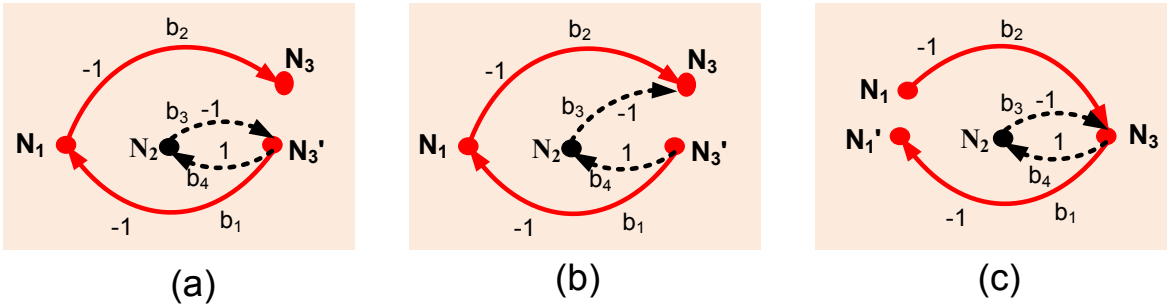


Fig. 4-9(a)&(c)Positive feedback loop breaking (b) Positive and negative feedback loop breaking

The mapping from the two break-vertices at vertex $\mathbf{N_3}$ to the corresponding break nodes in the circuit results in the open-loop circuits shown in Fig. 4-10. The excitations and responses needed for the break-loop voltage return method are also indicated.

An implementation of this circuit designed in a AMI 0.5um process was used for demonstrating representative simulation results. Device sizes of this implementation are shown in Fig. 4-8(a). The op amp was BRIEFLY DESCRIBE. The diodes have an area ratio of 8 in this circuit.

The simulated return maps for both open-loop circuits are shown in Fig. 4-11. Case 1 involves breaking only the positive feedback loop which shows the monotonic return map characteristics whereas for Case 2, both positive and negative feedback (NFB) loops are broken. In the latter case the transfer characteristic curve is non-monotonic. In this example, Case 2 more clearly shows the intersection points though both methods successfully identify the correct intersection points.

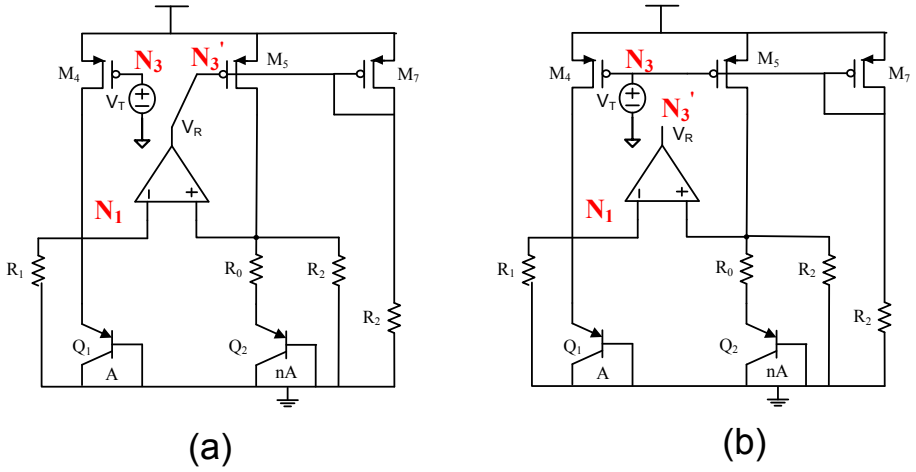


Fig. 4-10 Open loop amplifiers for homotopy analysis (a) intact NFB, (b) broken NFB

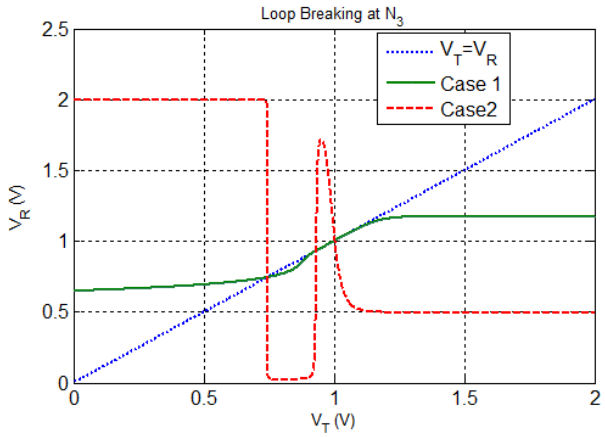


Fig. 4-11 Simulation results comparing different grouping

If a mistake is made in breaking the positive feedback loops the resultant return map will, in general, not be useful for identifying the equilibrium points. The simulation results shown in Fig. 4-12 were for the same circuit where the negative feedback loop was broken but where the positive feedback loop remained intact. In this example, the input was swept throughout the desired input range twice, once from small values to large values and once from large values to small values. The intact positive feedback loop produced hysteresis in the bidirectional sweep and neither the desired nor the undesired equilibrium point were detected.

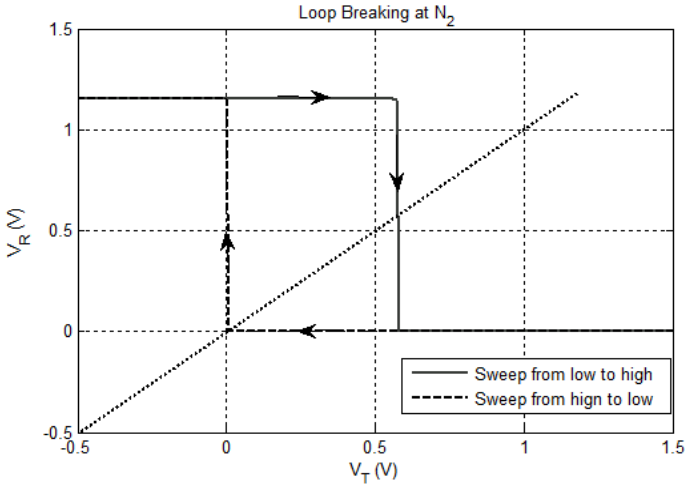


Fig. 4-12 Hysteresis situation

4.5.3. Simulation steps

The number of simulation steps required to identify the presence of a stable Trojan state with any of the homotopy methods discussed is dependent upon the circuit structure and on the implementation of the circuit. For the intact-loop methods it is also dependent upon where the excitation is applied to the circuit and for the break-loop methods it is dependent upon where and how the loop is broken. There are also variations in the number of simulation steps required from one circuit-level homotopy method to another. No attempt

will be made to identify the best homotopy method nor to determine how a particular homotopy method should be implemented. In this section a comparison of the homotopy methods will be made for two circuits with limited variants of how the homotopy methods are implemented to demonstrate that there can be significant differences in computational requirements when using circuit-level homotopy analysis for verifying the known presence of a stable Trojan state.

For the comparisons in this section, both the inverse Widlar and the Banba circuit were designed to operate in a AMI 0.5µ CMOS process. The device sizes for the two structures are given in Fig 4-7 and 4-8 respectively. For these implementations, the inverse Widlar test structure has two stable equilibrium points at V_{N1}=3.06 and V_{N1}=4.875V with 5V Vdd at 80ºC and the Banba has two stable equilibrium points at V_{OUT}=11.92uV and V_{OUT}=0.755V with 2V supply at 80ºC.

In these simulations, voltage steps were uniformly spaced on a linear axis with the first step at 0 and the last step at V_{DD}. Current steps were uniformly spaced on a logarithmic axis. The last current step was at the level expected for normal operation and the first step was established with an ad hoc trial and error approach and the simulation steps used in establishing the minimum current were not included in the step count. Simulations were made with the circuit simulator Spectre running in a Cadence environment.

Simulation results showing the number of steps required for four different homotopy methods are shown in Table 4-2 and Table 4-3 for Inverse-Widlar bias generator and the Banba bandgap reference respectively. The break points are not unique for break-loop analysis and the excitations points are not unique for intact-loop analysis. The specific break points and excitation points for the four different homotopy methods are shown in Table 4-5

and Table 4-6 for Inverse-Widlar bias generator and the Banba bandgap reference respectively. The Banba circuit has both a positive feedback loop and a negative feedback loop. The break points were selected so that only the positive feedback loop was broken and this resulted in a monotone return map. The symbol "X" placed in a row of the table indicates that the presence of both stable equilibrium points was not obtained with the number of steps corresponding to the designated row. The symbol "O" is the logical compliment of the symbol "X". The simulation results show that some circuit-level continuation method can find the Trojan operating points in fewer steps than other methods.

With the small sample size and with multiple options for break point and test signal insertion it is difficult to draw any conclusions about which homotopy methods are preferable. It can be observed from Table 4-3 that the break-loop voltage return method does perform better for this implementation of the Banba bandgap reference than the other methods used in the test.

Table 4-3 Simulation Steps for Inverse-Widlar

Homotopy method / Sweeping steps	Trojan State Detection Success(O)/Fail(X)			
	Intact loop		*Break loop*	
	Current return	**Voltage return**	**Current return**	**Voltage return**
3	X	X	X	X
5	O	X	X	X
8	O	X	X	O
10	O	O	O	O

Table 4-4 Simulation Steps For Bamba Bandgap Reference

Homotopy method / Sweeping steps	Trojan State Detection Success(O)/Fail(X)			
	Intact loop		*Break loop*	
	Current return	**Voltage return**	**Current return**	**Voltage return**
5	X	X	X	X
10	X	X	X	O
15	X	X	O	O
20	O	O	O	O

Table 4-5 Homotopy Test Circuits for Inverse Widlar Structure

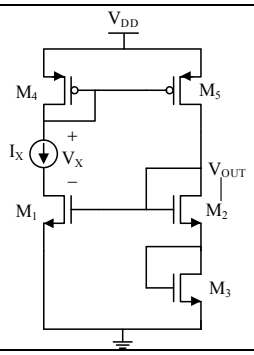
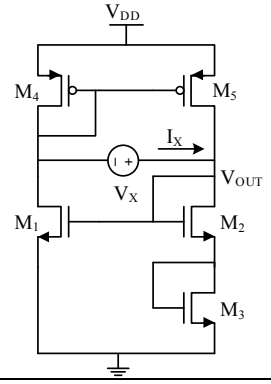
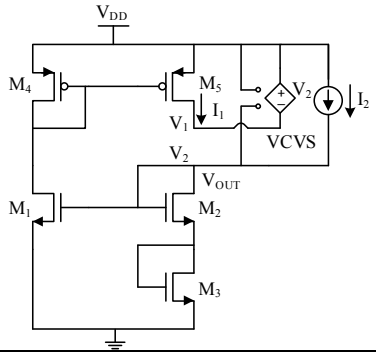
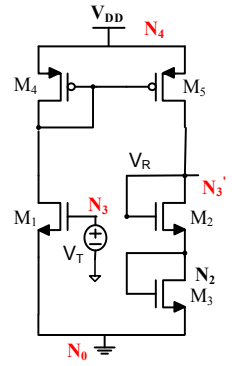
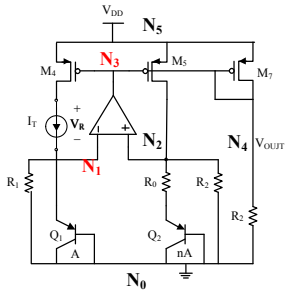
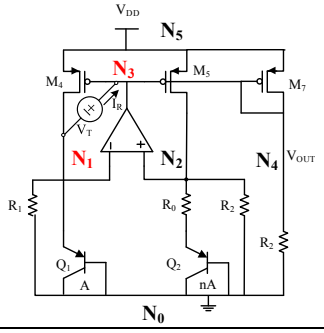
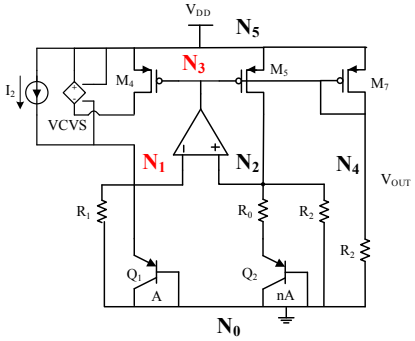
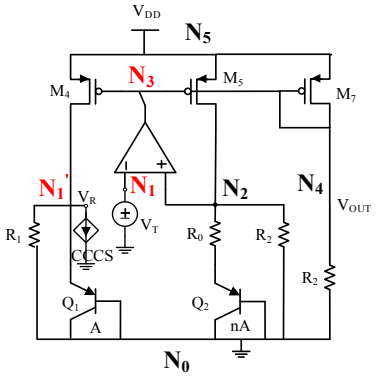
Homotopy Type	Circuit
Intact Loop Current Return	
Intact Loop Voltage Return	
Break Loop Current Return	
Break Loop Voltage Return	

Table 4-6 Homotopy Test Circuits for Banba Structure

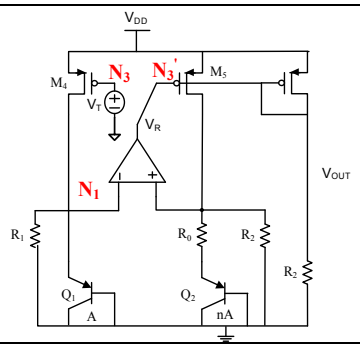
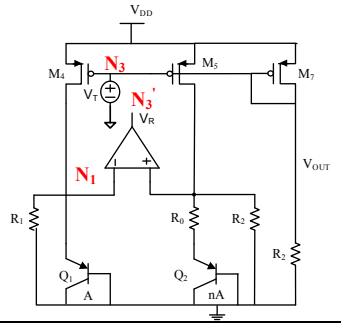
Homotopy Type	Circuit
Intact loop Current Return	
Intact loop Voltage return	
Break loop Current return	
Break loop Voltage return	

It is well-known that methods are available that can reduce computation time for finding solutions of monotonic functions. It was observed that if the negative feedback loop remains intact for a break-loop homotopy analysis of the Banba reference, then the return map will be monotone and, in the example considered previously. If the negative feedback loop is also broken when breaking the positive feedback loop, the return map will be non-monotone. A comparison of the number of simulation steps for the Banba circuit using the break-loop voltage return map has been made. The results appear in Table 4-7and the circuits used for this simulation appear in Table 4-8 . It can be observed that for this example the non-monotonic case requires fewer steps to find the presence of a Trojan operating point. A previous comparison of the same circuits depicted in Fig.4-10 also showed that the slope of the return map crossing point for the non-monotone response (case 2) is much larger than that for the monotone response (case1).

Table 4-7 Comparison between monotonic and Nonmonotonic

Transfer-Curve / **Sweeping steps**	**Trojan State Detection Success(O)/Fail(X)**	
	Non-monotonic	***Monotonic***
5	X	X
10	O	X
15	O	O
20	O	O

Table 4-8 Homotopy Test Circuits for Banba with Monotonic and Non-Monotonic Return Map

Homotopy Type	Circuit
Break loop voltage return (Special Case) • Monotonic • Break positive feedback loop	
Break loop voltage return • Non- monotonic • Break both positive and negative feedback loop	

4.6. Conclusion

Circuit-level homotopy methods can be used to identify all operating points in some useful circuits, can be used identify the need for a TSE (startup) circuit, and can be used to verify that the TSE is operating correctly. Both intact-loop and break-loop approaches were introduced. Because of the difficulty of identifying operating points that may be at extremely low current levels, linear voltage sweeping methods for both intact-loop and break-loop will circumvent the problem of determining lower bounds for logarithmic current sweeps.

An unanticipated outcome of this work is the recognition that a study of verification methods for identifying the presence of undesired stable equilibrium points in circuits that occasionally remain undetected by talented and conscientious design and verification engineers is closely related to the field of hardware security. More specifically, a large number of widely used analog and mixed-signal circuits are vulnerable to the adversarial insertion of analog hardware Trojans that can be extremely difficult to detect and that can have disastrous consequences when triggered. This work may have a direct bearing on recognizing where vulnerabilities exist for insertion of a class of insidious analog hardware Trojans and may lead to strategies for protecting society from the consequences of these Trojans.

CHAPTER 5 CONCLUSIONS

In conclusion, the research work is focused on the design of ultra-small on-chip temperature sensor that is suitable for multi-core on-line thermal monitoring. Also, a novel way to convert the analog signal to a digital output without traditional ADC and reference circuitry is designed, which has huge potential to save the area and power that can be utilized in the power/thermal management design. An analog verification method that can detect the effectiveness of the start-up circuit is established, rather than the traditional heuristic time-consuming method to exclude the start-up problem in a circuit, a systematic Homotopy method is built to successfully identify the existence of the multiple operating points in a circuit, and a startup circuit is needed to remove the unwanted DC operating point.

Chapter 2 proposes two all-CMOS accurate temperature sensor, which are designed for processor power management. The 5T temperature sensor consumes only 92μW and is featured with an extremely small area of 15μm×24μm in TSMC 0.18μm process. Nine chips fabricated in TSMC 0.18μm are tested under 1.8V voltage power supply. The performance of this sensor is highly linear within the temperature range [60°C, 90°C] working for power management and the temperature error is only -0.2°C ~0.6°C after one-point temperature calibration and batch slope error calibration. The 4T dual-threshold based temperature sensor with all cascade-biased circuitry is fabricated in IBM 130nm process features 60 μW with an area of 25μm×50μm. Five chips are tested under 1.2V supply, with one-point temperature calibration and batch slope error compensation, the chip performance achieved -0.18°C ~0.13°C temperature error which is also highly linear within the temperature range [60°C, 90°C]. Both temperature sensor has good accuracy for thermal control within processor

power management temperature range and it can accurately trigger temperature from 60°C to 90°C and protect processors from overheating.

Chapter 3 presents a compact CMOS temperature to digital converter without any reference generator or ADC. It has low power supply sensitivity, and can be used as temperature monitoring circuit to protect other on-chip circuits from over-heating with digital interface. A temperature trigger is designed using the fully cascade dual-threshold structure in Ch. 2 as the sensor core with a low offset comparator. The temperature–to-digital converter is closed-loop tested with an off-chip logic block. This design implemented in 0.13um process with 1.2V power supply. It works in the temperature range [60 ^{o}C, 90 ^{o}C] which is for power management purpose, and the measurement results show the maximum temperature error for the digital output in the operating range is ±0.1 ^{o}C.

Chapter 4 introduces a new method to verify the effectiveness of the start-up circuit. The traditional supply ramp method is ineffective at verifying effectiveness of a start-up circuit. The new circuit-level Homotopy method can identify all operating points in a circuit, and verify the need for start-up circuit. Four different methods for verifying the effectiveness of a start-up circuit at removing Trojan operating points were discussed. Although all successfully identified all operating states in the sample circuit considered here, this comparison suggests that some may be more practical than others for at least certain classes of circuits. Although the four Homotopy -method based approaches are effective at verifying removal of Trojan operating states, they will successfully identify all operating states in some of the more widely used circuits that may need start-up circuits for proper operation. This work suggests that the recognition of undesired stable equilibrium points in circuits may occasionally remain undetected by experienced design and verification engineers. Therefore,

a large number of widely used analog and mixed-signal circuits are vulnerable to the deliberate insertion of analog hardware Trojans that can be extremely difficult to detect and expose the circuit at high risk of Trojan attack. This work may have led to strategies for protecting society from the consequences of these Trojans.

REFERENCES

[1] R. McGowen, C.A. Poirier, C. Bostak, J. Ignowski, M. Millican, Parks, S. W.H.Naffziger, "Power and temperature control on a 90nm Itanium®-family processor," *IEEE J. Solid-State Circuits*, vol. 41, pp. 229-237, Jan. 2006.

[2] F.J. Mesa-Martinez, M. Brown, J. Nayfach-Battilana and J. Renau, "Measuring power and temperature from real processors," *IEEE Int. Symp. Parallel and Distributed Process.*, 2008, pp. 1-5.

[3] J. Shor, K. Luria and D. Zilberman, "Ratiometric BJT-based thermal sensor in 32nm and 22nm technologies." in *ISSCC Dig. Tech. Papers*, 2012, pp. 210-212.

[4] M.A.P. Pertijis, K.A.A. Makinwa, J.H. Huijsing, "A CMOS smart temperature sensor with a 3σ inaccuracy of ±0.1°C from -55°C to 125°C," *IEEE J. Solid-State Circuits*, vol. 40, no. 12, pp. 2805-2815, Dec. 2005.

[5] K. Souri,M. Kashmiri and K.A.A. Makinwa, "A CMOS Temperature sensor with an energy-efficient zoom ADC and an inaccuracy of ±0.25°C (3σ) from -40°C to 125°C", *ISSCC Dig. Tech. Papers*, pp. 310-311, Feb. 2010.

[6] F. Sebastiano, L.J. Breems, K.A.A. Makinwa, S. Drago, D.M.W. Leenaerts, B. Nauta, "A 1.2V 10μW NPN-based temperature sensor in 65nm CMOS with an inaccuracy of ±0.2°C (3s) from −70°C to 125°C," *IEEE J. Solid-State Circuits*, vol.45, no.12, pp.2591-2601, Dec. 2010.

[7] K. Souri, K.A.A. Makinwa, "A 0.12 mm^2 7.4μW micropower temperature sensor with an inaccuracy of ±0.2°C(3σ) from -30 °C to 125°C," *IEEE J. Solid-State Circuits*, vol.46, no.7, pp.1693-1700, July 2011.

[8] P. Chen, C.-C. Chen, C.-C. Tsai, W.-F. Lu, "A time-to-digital-converter-based CMOS smart temperature sensor," *IEEE J. Solid-State Circuits,* vol.40, no.8, pp.1642-1648, Aug. 2005.

[9] P. Chen, C.-C. Chen,Y.-H. Peng, k.-M. Wang, Y.-S. Wang, " A time-domain SAR smart temprature sensor with curvature compensation and a 3σ inaccuracy of -0.4°C~0.6°C over a 0°C to 90°C Range," *IEEE J. Solid-State Circuits,* vol.45 no.3, pp.600-609, Mar. 2010.

[10] K. Luria and J. Shor, "Miniaturized CMOS Thermal Sensor Array for Temperature Gradient Measurement in Microprocessors" *in Proc. ISCAS* 2010, pp. 1855-1858.

[11] T. Yang, S. Kim, P.R. Kinget, M. Seok, " 0.6-to-1.0V 279μm^2, 0.92μW temperature sensor with less than +3.2/-3.4°C error fpr on-chip dense thermal monitoring," in *ISSCC Dig. Tech. Papers*, 2014, pp. 282-284.

[12] M. Law, A. Bermak, and H. Luong, "A Sub-W Embedded CMOS Temperature Sensor for RFID Food Monitoring Application", *IEEE J. Solid-State Circuits*, pp. 1246 – 1255, Jun. 2010.

[13] S.-H. Lee, C. Zhao, Y.-T. Wang, R. Geiger and D. Chen, "Multi-Threshold Transistors Cell for Low Voltage Temperature Sensing Applications," *IEEE Int. Midwest Symp. Circuits Syst.,* Aug. 2011.

[14] V. Szekely, C. Marta, Z. Kohari and M. Rencz, "CMOS sensors for on-line thermal monitoring of VLSI circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 5, no. 3, pp. 270-276, Sept. 1997.

[15] C. Zhao, Y.-T. Wang, D. Genzer, D. Chen, R. and Geiger, "A CMOS on-chip temperature sensor with -0.21°C 0.17 °C inaccuracy from -20 °C to 100 °C," *in Proc. ISCAS* 2013, pp. 2621-2625.

[16] N. Maghari, O. Shoaei, "A dynamic start-up circuit for low voltage CMOS current mirrors with power-down support," *in Proc. ISCAS,* 2005, pp. 4265- 4268.

[17] B. Yuan, Lai X., H. Wang ,Y. Wang, "The design of a start-up circuit for boost DC-DC converter with low supply voltage," *Proc. 6th Int. Conf. ASIC*, 2005, pp.483-487.

[18] V. C. Tuan , D.T. Wisland, T.S.Lande, F.Moradi, Y. H. Kim; , "Novel start-up circuit with enhanced power-up characteristic for bandgap references," *IEEE Int. SOC Conf.*, , 2008, pp.123-126.

[19] B.H. Stark, G.D. Szarka, E.D. Rooke, "Start-up circuit with low minimum operating power for microwatt energy harvesters," *IET Circuits, Devices & Syst.*, vol.5, no.4, pp.267-274, July 2011.

[20] R. Jacob Baker, Harry W.Li and Davis E.Boyce: "CMOS Circuit Design, Layout and Simulation ", 3rd. Wiley, 2010 pp. 624-625

[21] B. Razavi, "Design of Analog CMOS Integrated Circuits", McGraw-Hill, 2001.

[22] X. Xi, M. Dunga, J. He, W. Liu and C. Hu, BSIM4.3.0 MOSFET Model Users' Manual. Berkeley, CA: Univ. California, 2003, pp. 119.

[23] G.C. M. Meijer, G. Wang, F. Fruett, "Temperature sensors and voltage references implemented in CMOS technology," *IEEE J. Sensors*, vol. 1, no. 3, pp. 225-234, Oct. 2001.

[24] W. Wang, V. Reddy, A.T. Krishnan, R. Vattikonda, S. Krishnan, Y. Cao, "Compact modeling and simulation of circuit reliability for 65-nm CMOS technology," *IEEE Trans. Device Mater. Rel.*, vol.7, no.4, pp.509-517, Dec. 2007.

[25] E. Maricau, P. De Wit, G. Gielen, "An analytical model for hot carrier degradation in nanoscale CMOS suitable for the simulation of degradation in analog IC applications," *Microelectronics Rel.*, vol. 48, no. 8–9, pp. 1576-1580, 2008.

[26] N.D. Arora, M.S. Sharma, "MOSFET substrate current model for circuit simulation," *IEEE Trans. Electron Devices*, vol. 38, no. 6, pp. 1392-1398, Jun. 1991

[27] M. A. Alam, S. Mahapatra, "A comprehensive model of PMOS NBTI degradation," *Microelectronics Rel.*, vol. 45, no. 1, pp. 71-81, 2005.

[28] S. Bhardwaj, W. Wang, R. Vattikonda, Y. Cao,S. Vrudhula, "Scalable model for predicting the effect of negative bias temperature instability for reliable design," *IET Circuits, Devices & Syst.*, vol.2, no.4, pp.361-371, Aug. 2008.

[29] J. R. Hoff, R. Arora, J. D. Cressler, G.W. Deptuch, P. Gui,N.E. Lourenco, G. Wu, R. J. Yarema, "Lifetime studies of 130nm nMOS transistors intended for long-duration, cryogenic high-energy physics experiments," in *IEEE Nucl. Sci. Symp. and Medical Imaging Conf.,* 2011, pp.685-693.

[30] M. Sasaki, M. Ikeda, and K. Asada, "A temperature sensor with an inaccuracy of −1/ +0.8 °C using 90 nm 1-V CMOS for online thermal monitoring of VLSI circuits," IEEE Trans. Semicond. Manuf., vol. 21, no. 2, pp. 201–208, May 2008.

[31] S. A. Jawed, W. A. Qureshim A. Shafique, J. A. Qureshi, A. Hameed, M. Ahmed, "Low-power area-efficient wide-range robust CMOS temperature sensors," *Microelectronics J.,* vol.44, no. 2, Feb. 2013.

[32] P. R. Grey, etc., "*Analysis and Design of Analog Intergrated Circuits,"*

[33] G.C.M. Meijer and J.B. Verhoeff, , "An Integrated Bandgap-Reference," *Solid State Circuits Conf. (ESSCIRC), 1975 First European* , pp.40-41, 2-5, Sept. 1975

[34] R.M. Fox and M. Nagarajan, "Multiple operating points in a CMOS log-domain filter," in *Proc. IEEE Int. Symp. Circuits Systems,* vol.3, pp.689-692, Jul 1999

[35] L.B. Goldgeisser and M.M. Green,"A novel algorithm that finds multiple operating points of nonlinear circuits automatically," in *Proc. IEEE Int. Symp. Circuits Systems* vol.3, pp.558-561, Jun 1998

[36] R.C. Melville, L. Trajkovic, S.-C. Fang and L.T. Watson, "Artificial parameter homotopy methods for the DC operating point problem," *IEEE Trans. Computer-Aided Design*, vol.12, no.6, pp.861-877, Jun 1993

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

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

[39] M.M. Green and A.N.Jr. Willson, "How to identify unstable DC operating points," *IEEE Trans. Circuits Syst.-I,* vol.39, no.10, pp.820-832, Oct 1992

[40] M. Tadeusiewicz, "A method for identification of asymptotically stable equilibrium points of a certain class of dynamic circuits," *IEEE Trans. Circuits Syst.-I,* vol.46, no.9, pp.1101-1109, Sep 1999

[41] H. Wen and M. M. Green, "Use of a continuation method for analyzing startup circuits," in *Proc. IEEE Int. Symp. Circuits Systems*, pp.1527-1530, May 2010

[42] L. Han, Y. Wang, X. Zhang, Y.Dai and Y. Lu, "A simple and effective method to achieve the successful start-up of a current reference," *J.of Semiconductors*, vol.2, no.8, 2012

[43] Y.-T. Wang, C. Zhao, R. L. Geiger, D. Chen and S.-C Huang, "Performance verification of start-up circuits in reference generators," *IEEE Int. Midwest Symp. Circuits Systems,* pp.518-521, Aug. 2012

[44] 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 J. Solid-State Circuits*, vol. 34, pp.670 -674, 1999

[45] M. Yuffe, E. Knoll, M. Mehalel, J. Shor and T. Kurts, "A fully integrated multi-CPU, GPU and memory controller 32nm processor," in *ISSCC Dig. Tech. Papers*, 2011, pp. 264-266

[46] M. J. M. Pelgrom, A. C. J. Duinmaijer and A. P. G. Welbers, "Matching properties of MOS transistors," *IEEE J. of Solid-State Circuits*, vol. 24, no. 5, pp. 1433-1439, Oct 1989.