AN FPGA NOISE RESISTANT DIGITAL TEMPERATURE SENSOR WITH AUTO CALIBRATION

THESIS

Brandon A. Brown, Second Lieutenant, USAF

AFIT/GCE/ENG/12-02

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GCE/ENG/12-02

AN FPGA NOISE RESISTANT DIGITAL TEMPERATURE SENSOR WITH AUTO CALIBRATION

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Computer Engineering

Brandon A. Brown, B.S.C.E.

Second Lieutenant, USAF

March 2012

AFIT/GCE/ENG/12-02

AN FPGA NOISE RESISTANT DIGITAL TEMPERATURE SENSOR WITH AUTO CALIBRATION

Brandon A. Brown, B.S.C.E.
Second Lieutenant, USAF

Approved:

//signed//	22 February 2012
Maj Todd R. Andel, PhD Chairman	Date
//signed//	22 February 2012
Lt Col LaVern Starman, PhD Member	Date
//signed//	22 February 2012
Maj Mark D. Silvius, PhD Member	Date

AFIT/GCE/ENG/12-02

Abstract

In recent years, thermal sensing in digital devices has become increasingly important. From a security perspective, new thermal based attacks have revealed vulnerabilities in digital devices. Traditional temperature sensors using analog-to-digital converters consume significant power and are not conducive to rapid development. As a result, there has been an escalating demand for low cost, low power digital temperature sensors that can be seamlessly integrated onto digital devices. This research seeks to create a modular Field Programmable Gate Array digital temperature sensor with auto one-point calibration to eliminate the excessive costs and time associated with calibrating existing digital temperature sensors. In addition, to support the auxiliary protection role, the sensor is evaluated alongside a RSA circuit implemented on the same chip, with methods developed to mitigate noise and power fluctuations introduced by the main circuit. The result is a digital temperature sensor resistant to noise and suitable for quick mass deployment in digital devices.

Acknowledgements

First, I would like to my Lord and Savior, Jesus Christ, for the many blessing in my life, as well as the talents and abilities that have enabled me to complete my Master's Degree. I would like to thank my wonderful wife for her support and encouragement. I would also like to thank my advisor, Major Todd Andel, for his guidance and direction through my research. Finally, I would like to thank my VLSI labmates for their constant distractions, sarcastic reviews, perilous lunches, and friendship.

Brandon A. Brown

Table of Contents

Page

List of Figures

Figure Page

List of Tables

AN FPGA NOISE RESISTANT DIGITAL TEMPERATURE SENSOR
WITH AUTO CALIBRATION

I. Introduction

Over the past few decades, our culture has become increasingly dependent on digital technologies. A typical person in the US may have two computers, a tablet device, and a mobile phone, all connected to each other and the rest of the world. Business, entertainment, and even social groups are now reliant on cyberspace.

In the excitement of advancing technology, security has struggled to keep up [9]. In the digital race to produce the next greatest technology first, security is often left as a future patch or left for the next device. While this level of security may be accepted in the commercial realm, it is unacceptable for national defense. To maintain its position as the leader in air, space, and cyberspace, the U.S. Air Force must be on the leading edge of security.

Vulnerabilities in the DoD's devices can have exponentially worse consequences than vulnerabilities in typical commercial products. While commercial vulnerabilities may lead to angry users and lost profits, vulnerabilities in defense products can allow an adversary to exploit critical technology, which include obtaining sensitive information, neutralizing defense systems, or, most importantly, reverse engineer devices.

Once a device has been reverse engineered, an adversary can then replicate the device, mitigating the technological advantage of the United States. Therefore, protection of United States critical technologies is crucial in order to maintain its edge on the battlefield. Deputy Attorney General James Cole recently stated, "Intellectual property is one of America's greatest assets and protection of these assets is vital to

our economy, our health, and our legacy." [10]

As DoD attempts to reduce its development time of new technologies, the Field Programmable Gate Array (FPGA) has become a very appealing device for embedded systems. As the name implies, FPGAs are able to be reprogrammed after fabrication to suit a wide variety of functions, such as digital signal processing, parallel processing, etc. FPGAs permit a new hardware design to be simply downloaded onto the device in minutes, as compared with months of fabricating an Application Specific Integrated Circuit. Moreover, FPGAs allow hardware to be realized at a fraction of the cost.

As FPGAs become more standard, adversaries will focus on exploiting them. Currently, little research has been done on identifying vulnerabilities of FPGAs, and even less on securing them. One such vulnerability involves exposing FPGAs to extreme temperatures, which can cause critical memory contents, such as encryption keys, to be revealed or modified. This research focuses on protecting FPGAs from thermal attacks.

1.1 Problem Statement

To protect an FPGA from thermal attacks, it must be able to discreetly monitor temperature changes. Traditional temperature sensors measure the base-emitter voltages of bipolar transistors, which varies with temperature [11, 12]. These voltages must be measured using an analog-to-digital (ADC) converter. While these analog sensors have proven reliability and a high degree of accuracy, the expense is large area and significant power consumption due to the ADC, preventing their adoption in mobile devices. These sensors also require separate design and fabrication since they are not compatible with the Complementary Metal Oxide Semiconductor (CMOS) process. These problems are additionally compounded if many sensors are desired to characterize a larger area on the chip.

Fully digital temperature sensors based on the correlation between integrated circuit propagation delay and core temperature are much more suitable for defense applications. It has generally been assumed that while a digital temperature sensor is smaller and more efficient than its analog counterparts, that it does so at the expense of accuracy [3]. However, many of the latest designs have accuracies within reach of a typical analog sensor and are more than adequate for circuit protection. A digital temperature sensor's small size and low power allow for many sensors to be placed on a single chip, even in mobile devices. An all digital approach allows for easy integration with Very Large Scale Integration (VLSI) systems and even dynamic insertion and removal in programmable logic devices such as FPGAs. In the case of security systems, digital sensor implementations are much more difficult to detect and disable since they are integrated and dispersed within the device. Thus, digital temperature sensors are an ideal candidate for thermal circuit protection.

1.2 Research Goals and Hypothesis

1.2.1 Goals.

The main goal of this research is to design an improved digital temperature sensor for thermal circuit protection and determine the accuracy and modularity when implemented on FPGAs. Two primary goals are to develop auto calibration and noise resistance. Auto calibration enables rapid mass calibration of many sensors outside the lab environment, reducing the time and cost of high volume deployment and permitting operation in the field. Noise resistance involves studying the effects of additional components and implement measures to mitigate any adverse effects. Since digital temperature sensors are designed to protect a main circuit, they must be resistant to noise and power fluctuations due to other components.

1.2.2 Hypothesis.

The research hypothesis is that auto calibration using one temperature point provides reasonable accuracy to be used in circuit protection, while significantly reducing the deployment time of the sensor. Additionally, it is expected that the digital temperature sensor is negatively affected while a main component is running, yet a modified calibration is able to correct any offset noise from the additional component.

1.3 Thesis Organization

This chapter presented the problem of thermal attacks on FPGAs and the goal of designing a digital temperature sensor for thermal circuit protection. Chapter 2 provides background information on thermal attacks and digital temperature sensors. Chapter 3 describes the research methodology and experimental setup. Chapter 4 presents the design and results of the digital temperature sensor. Finally, Chapter 5 concludes with a summary, contributions, and recommended future work.

II. Background

In this chapter, background information is presented to give context to the research. First, description of modern thermal attacks are presented. Then, the basic design of a digital temperature sensor is presented. Finally, significant improvements of digital temperature sensors are reviewed, focusing on accuracy, calibration techniques, and noise tolerance.

2.1 Thermal Attacks

In the last decade, adversaries have exploited integrated circuits' sensitivity to temperature. Thermal attacks are cheap, quick, and use everyday materials. While it normally requires physical access to the device, it is surprisingly easy to use both extreme heat or below-freezing temperatures to either modify the circuit or retrieve memory contents that could potentially leak a key used for cryptography.

It is well known that extreme heat can degrade the performance or significantly lower the reliability of electronic devices [13]. Many basic thermal attacks attempt to use malicious code to self-heat the device. One such study [14] focuses on presenting the failures of conventional thermal management schemes in defending against these thermal attacks. Typical thermal management systems employ only a few sensors to characterize the average heat or monitor only the expected hot spots, leaving those small, unexpected, yet important areas vulnerable to heat attacks. The study experimented with heating up the instruction cache of an Alpha 21364 Processor using continuous NOP instructions - an instruction that does not use any functional units of the processor, and therefore will not trigger the thermal management. An easy defense against such an attack would be to increase the number of thermal sensors. However, this solution would only be practical with extremely small, low

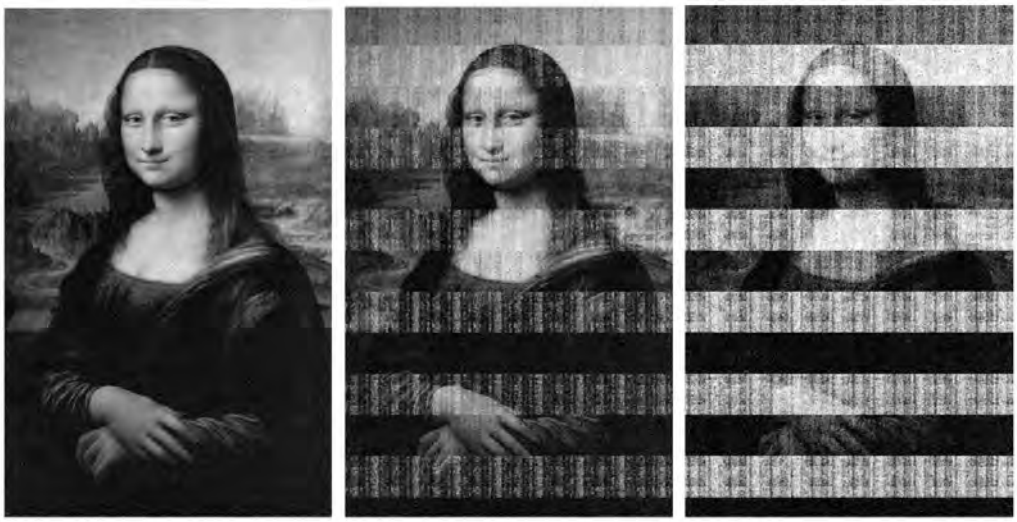
power sensors, such as all digital temperature sensors.

Another study looked at the affects of heat on different memory structures [15]. Electrically Erasable Programmable Read-Only Memory (EEPROM) and Flash memory are built using floating gate transistors to store bits, and predicted lifespan is around 40 and 100 years, respectively. Using lasers to heat the memory, it was found that temperatures of 450 degrees Celsius were able to cause the memory cells to lose their charge, which effectively sets the memory bit to zero. Also, the longer the exposure, the more bits were affected, up to a certain point. This discovery leaves cryptographic keys vulnerable to a thermal attack, since an adversary with knowledge of where the key is stored could change the key to all 0's, and break the encryption.

A more practical thermal attack, requiring nothing more than a canister of multi-purpose duster, was shown in a study by Princeton University [1]. The thermal attack is based on the principle that dynamic memory devices retain data longer under low temperature, even after power loss. The research group used the canister upside down to freeze Dynamic Random Access Memory (DRAM) from a typical laptop down to -50 degrees Celsius. Then, the power was cut, and the DRAM was connected to a separate machine for analysis. While DRAM will lose its memory contents after several seconds at room temperature without power, the low temperature gave sufficient time to transfer a large percentage of the data [1]. Figure 1 shows a visualization of memory decay after being frozen. Several popular disk encryption schemes, including TrueCrypt and BitLocker, were defeated using this basic thermal attack.

2.2 The Digital Temperature Sensor

In the past decade, thermal sensing in digital devices has become increasingly important. In the commercial realm, increasing processing power has led to increased heat and the need for thermal management schemes. From a security perspective,



(a) Image after 5 sec. (b) Image after 30 sec. (c) Image after 60 sec.

Figure 1. Visual example of memory decay [1]

thermal detection has become necessary to protect against recent thermal-based attacks on digital devices. As a result, there has been an escalating demand for low cost, low power temperature sensors that can be seamlessly integrated onto digital devices. These sensors, known as digital temperature sensors, are well suited for circuit protection and are the focus of this research.

Digital temperature sensors are based on the correlation between the logic propagation delay of integrated circuits and core temperature. Within a nominal range as core temperature rises, delay rises nearly linearly. Thus, digital temperature sensors measure the delay of a circuit path to infer the temperature. Typically, a ring oscillator is used to measure delay. A ring oscillator consists of an odd number of inverters connected in series that loops back to its input, creating a circular chain that oscillates with a period given in the following equation (the summation of the rise and fall times of each device):

$$T_{osc} = N(T_{PHL} + T_{PLH}) \tag{1}$$

T_{osc} = Oscillation Period

N = Number of Inverters

T_{PHL} = Inverter Falling Delay Time

T_{PLH} = Inverter Rising Delay Time

The basic digital temperature sensor, first proposed in [2], is shown in Figure 2.

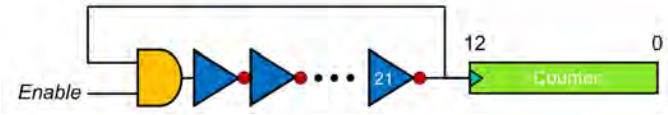


Figure 2. Ring oscillator

To measure temperature, the ring oscillator is timed against a reference clock and the number of oscillations stored by a digital counter. Calibration is necessary to correlate the number of oscillations with a reference temperature. Also, because each device is unique at the physical level, calibration is also unique to each device. At 2.5 volts, the relationship between delay and temperature is almost perfectly linear, as seen in Figure 3.

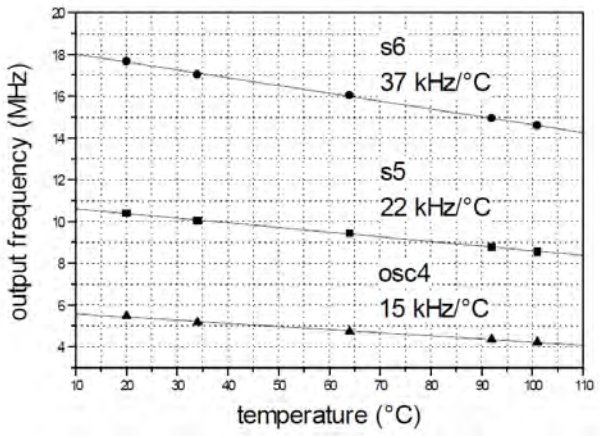


Figure 3. Ring oscillator frequency vs temperature at 2.5v [2]

However, as Moore's Law continued and feature size continued to shrink, voltages also dropped. Additional experiments with ring oscillators found that lower voltages

impacted delay more significantly, and the relationship was not quite as linear, as shown in Figure 4.

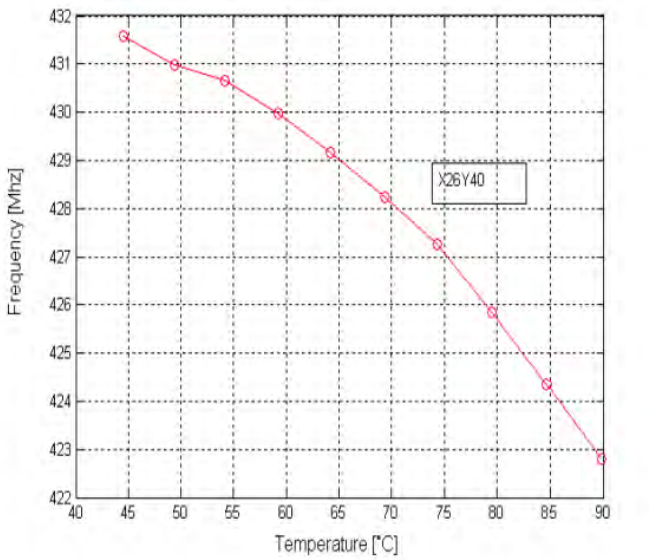


Figure 4. Ring oscillator frequency vs temperature at 1.0v [2]

From this basic design, a generic layout has been proposed to characterize the function of an all-digital temperature sensor, shown in Figure 5. The two main components are the Temp-to-Pulse generator and the cyclic Time-to-Digital Converter (TDC). The former component is composed of a delay line to generate a pulse, where the width of the pulse is proportional to the temperature. A delay line is any circular logic that is sensitive to temperature, typically a ring oscillator as discussed above. The second component, the cyclic time-to-digital converter, digitally encodes the pulse width to represent a temperature measurement. In the basic design, a counter can suffice for the TDC component.

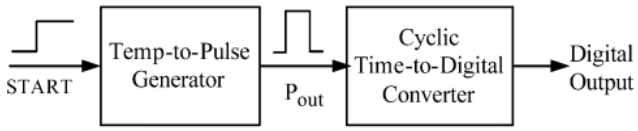


Figure 5. Basic layout of digital temperature sensor [3]

2.3 Improving the Sensor

Since the ring oscillator was first used to measure temperature, there have been several improvements of the basic temperature sensor. The following reviews the advances in the critical areas of accuracy, calibration, and noise tolerance.

2.3.1 Accuracy.

It has generally been assumed that while a digital temperature sensor is smaller and more efficient than its analog counterparts, that it does so at the expense of accuracy [3]. However, many of the latest designs boast accuracy just as good as many analog sensors and within reach of the best.

It has been established that accuracy improves with the length of the delay since the minuscule temperature dependence of delay is amplified over a longer period of time [16]. To retain minimal area with a sufficiently long delay time, a time amplifier is proposed in [16]. The time amplifier connects the delay line to a counter to circulate the delay line a given number of times, similar to a ring oscillator.

Obviously the shorter the delay line, the less area the sensor utilizes. However, a shorter delay line requires more circulations to achieve the same overall delay time, increasing the risk of self-heating. Self-heating occurs when the sensor's delay line accumulates heat since the time between each propagation for a given inverter is too low. Thus, the delay line length and circulation count should be balanced with area and accuracy requirements.

Accuracy becomes a much more difficult problem at lower voltages. As previously discussed, lower voltages affect the linear relationship between frequency and temperature. To mitigate the effect of low voltages, the number of inverters in the ring oscillator can be increased. Of course, the trade-off is additional area. Using standard deviation as a metric, [4] measured frequency of a ring oscillator from 0.95 to 1.05

volts using a variable number of inverters. The result is shown in Figure 6, from which the authors conclude that 25 inverters is the optimum number for reasonable accuracy while retaining a small size on the chip. Of course, the optimum number may vary according to size of the specific device as well as accuracy requirements.

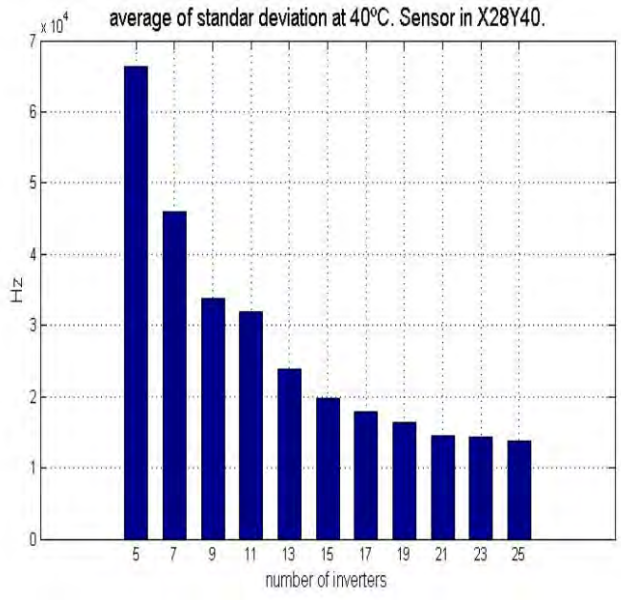


Figure 6. Standard deviation of oscillation frequency at 40 °C [4]

One proposed design takes the basic ring oscillator and replaces inverters with complex gates [17]. The ideal way to achieve linearity would be to adjust the physical transistors in the inverters. However, this approach would require a custom built device, preventing the design from being seamlessly integrated in FPGAs. By using complex gates, the authors assert that the additional transistors would mitigate the variation between the gates in the ring oscillator, and thus the curve would be more linear.

2.3.2 Precision.

Prior research has found digital temperature sensors are very stable at constant voltages. However, stable voltage requires inconvenient lab-quality power supplies.

Small variations from common power supplies, such as a battery or household outlets, can cause fluctuations based on the voltage dependency previously discussed. These fluctuation cause the precision of the sensor to decrease. A simple, effective solution to mitigate these fluctuations is to average the sensor readings. In [5], the authors attempt to find the optimal number of averaging points to increase precision. The graph of their findings is shown in Figure 7.

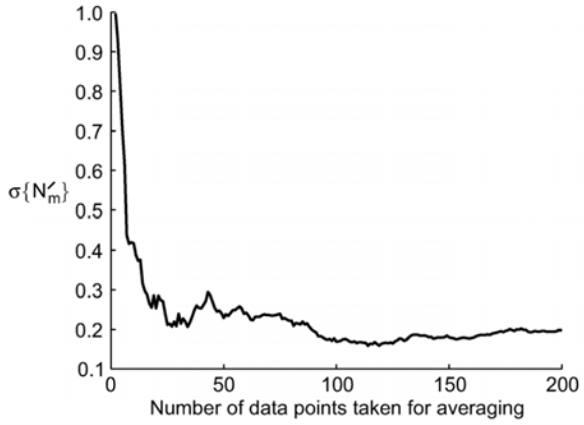


Figure 7. Standard deviation of averaged temperature at 30 °C vs number of averaged data points [5]

The study concludes that the precision increases up to 100 data points, after which the time correlation adds to the error. The only downside of increasing the number of data points is the decreased sampling rate and increased energy consumption. However, even with just a few averaging points, the precision remains within one standard deviation, sufficient for the majority of uses. Thus, the precision of digital temperature sensors is excellent, and can be increased further with averaging if the energy and time requirements are met.

2.3.3 Calibration.

One key issue for digital thermal sensors is calibration, which goes hand in hand with accuracy. Since digital thermal sensors are integrated directly on the device,

they are subject to the process variations in the CMOS fabrication that make each device unique at the physical level. While each device will logically function the same, the minuscule differences in transistor sizes and wire lengths directly affect its delay, and thus each will have a unique correlation to temperature. Therefore, calibration aims to find the coefficients for the equation that relates delay and temperature in each device.

Currently, most digital thermal sensors use rudimentary methods to calibrate the device. In the case of [2], a specific FPGA with a digital temperature sensor is calibrated by recording counter values for the entire range of temperatures needed, using a temperature chamber. Then, the equation is found using statistical regression. While very accurate, this method requires several hours to profile a single device, inhibiting mass deployment of the system.

To achieve low cost and mass deployment, several recent efforts have been devoted to reducing calibration time and cost. One fairly simple approach is to set the initial temperature, and record the digital output. Then, using this offset, the temperature can be calculated for any digital output [18]. While extremely quick, this method generates a large error by assuming a linear response, where all the devices have an identical slope on the delay vs. temperature curve.

Two point calibration, used in [19, 20, 21, 3, 22, 23, 24], reduces time by requiring only two different temperature points to calibrate out process variation stemming from device fabrication. While more efficient than a complete calibration over an entire temperature range, two-point calibration is still too tedious and time consuming, especially if a large number of sensors are utilized on a chip.

The latest designs attempt to operate with one-point calibration. One-point calibration loses some accuracy, but the trade-off is much easier and quicker calibration, substantially decreasing the time and cost of calibration many sensors. One

such device achieves one-point calibration using dual-delay-locked-loops (DLLs) to calibrate the digital temperature sensor [19]. The calibration circuit normalizes the temperature-to-pulse delay to the reference DLL delay by using multiplexors to select the number of inverters in the delay line until the two match. The design attempts to normalize the digital outputs of all devices, so that each device will output the same code for any given temperature. However, the design has two major downfalls: The DLLs require a substantial increase in chip area and power [20]; also, the device is custom fabricated, negating much of the time and cost benefits of one-point calibration since fabrication is significantly more expensive and time consuming than implementation on an FPGA.

A newer design in [6] attempts to meet the same goal of normalizing delay, yet without a significant increase in area or power. The design is an extension of their previous work of improving accuracy, by increasing the pulse width, by using a fixed multiplier [3]. This newer design modifies that circuit to use a variable multiplier, which is adjusted by a calibration circuit. The block diagram of the circuit is shown in Figure 8.

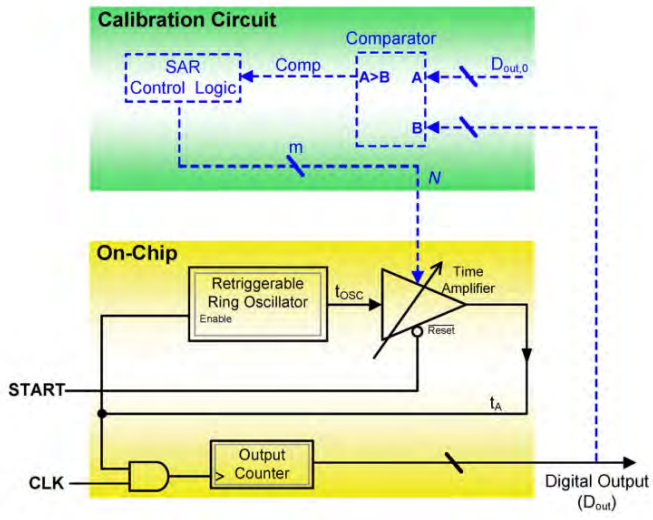


Figure 8. Auto calibrated proposed digital temperature sensor [6]

One point calibration is made possible by the variable multiplier. At the calibration temperature, the multiplier of each sensor is adjusted so the output is uniform across all sensors at any given temperature. The calibration circuit is implemented off chip to save space, and removed after initial calibration.

2.3.4 Noise Tolerance.

One particular concern with digital temperature sensors is the impact from other processing in proximity. While digital temperature sensors are extremely useful, they are normally not the main program on the device and thus are subject to noise. Since digital temperature sensors are based on delay from primitive logic, it is crucial that other processing does not affect the delay or alter the calibration of the device. Another source of noise may be from the power supply. As seen earlier, voltage has a small effect on oscillation frequency, which may be interpreted incorrectly as a change in temperature, when in fact the change may be due to a power supply variation.

The simple solution to the noise problem is to utilize a large number of sensors both in one spot, as well as spread out over the entire physical area of the chip [25]. In the case of an FPGA, this method requires using the advanced tools to specify the location of components. Using this scheme, taking the average temperature can help filter out noise on isolated hot spots. However, the average may actually mask true thermal extremes that are concentrated in a specific area on the chip.

A more complex solution is presented in [25]. The study focuses on statistical approaches to characterize the integrity of sensors. Monte Carlo simulations are used to develop a probability density function of the range of frequencies possible for certain temperatures given a randomness in fabrication. The goal is to develop an expected frequency for a given temperature. In addition, the study computes a correlation coeffecient between different components on the device, where the distance is used

as the correlation metric. The theory is that a temperature reading in a certain area should have similar readings to other sensors in close proximity. There should exist a downward trend from the center of a hotspot outwards to the rest of the chip. The effect is similar to a low-pass filter, which should increase the integrity of the temperature profile.

2.3.5 Placement on FPGA.

One particular question that arises with digital temperature sensors is how many are required and where should they be placed? A device such as an FPGA has many components that create different hot spots. Thus, a single sensor, even if it is extremely accurate, may not represent the die temperature and certainly cannot give a complete thermal profile of the device. One study looks at the minimum number of digital temperature sensors required to optimally measure all the hotspots of an FPGA [7]. The naive solution is to determine the range of a sensor (i.e., the range it can accurately detect a change in temperature) and create a grid over the FPGA. While this method works reasonably well, it requires many sensors, some of which are unnecessary. The optimal placement, on the other hand, uses a Recursive Bisection algorithm to allocate sensors to cover as many hotspots as possible. As long as the hotspots are known, it allows for optimal coverage of the FPGA while using minimal area. Figure 9 shows a comparison of the two methods.

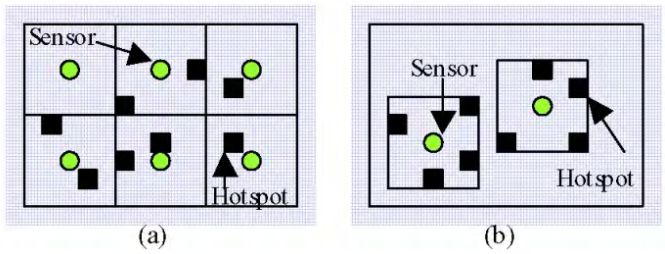


Figure 9. Two different digital temperature sensor placement algorithms: (a) Grid placement (b) Optimal Placement [7]

2.4 Summary

Integrated circuits' sensitivity to temperatures has opened up another avenue for adversaries to exploit. Freezing temperatures can slow the memory loss of dynamic memory, allowing crucial data to be accessed after power loss. Extremely hot temperatures can degrade electronic components and alter memory contents. Digital temperature sensors are the ideal solution to detecting temperature changes. Their small, low power nature allows many of them to be easily placed on integrated circuits, specifically FPGAs.

The first design of a digital temperature sensor was simply a ring oscillator connected to a counter. Substantial improvements have been made to the basic design, increasing the accuracy and precision. Calibration improvements have gone from a complete profiling to two-point and even one-point calibration, reducing time and costs. One outstanding issue yet to receive much attention is the digital temperature sensors performance when running concurrently with a main entity on the same chip. Other than utilizing more sensors with some signal filtering, little research has been devoted to noise resistance. Still, with all the improvements, digital temperature sensors are a promising replacement for traditional analog sensors, especially for circuit protection schemes.

III. Methodology

This chapter presents the research methodology. The approach to meet the research goals is presented, along with a descriptions of the system boundaries and services. Specific metrics to characterize the sensor are discussed, as well as different parameters and factors that are varied in the experiments. A thorough description of the experimental setup and evaluation technique is documented. Finally, the chapter ends with a summary of the methodology.

3.1 Approach

A pulse based measuring scheme is proposed rather than the typical oscillator counter previously shown. A pulse based design measures the time for the ring oscillator to reach a variable number of circulations, rather than count the number of oscillations in a given time period. The former is more precise since it eliminates potential residual delay not counted if the circulation has not completed. Time is measured by creating a pulse whose width is proportional to the oscillation time. This pulse is digitally encoded using the system clock as a reference.

The variable number of circulations, also known as the gain, allows for auto calibration. This automatic one-temperature-point calibration meets the goal of modularity, since a single design can be implemented on any FPGA and each digital temperature sensor can simultaneously quickly calibrate to its particular FPGA. Moreover, one-point calibration does not require thermal equipment, and therefore the sensor calibration is not confined to the lab environment. Thus, auto calibration significantly reduces the time and cost of high volume deployment, permitting operation in the field and allowing for a highly modular digital temperature sensor.

Since the digital temperature sensor is meant to supplement a main entity, it

is crucial that the sensor be immune to the main entity's electric noise and power fluctuations. That is, a sensor's accuracy should be no worse in the presence of noise. A 512-bit RSA circuit is used in this research as the main entity. To increase the sensor's resistance to noise, two different approaches are explored. The first method involves halting all other computations during the sensors readings, while the second uses an extension of the auto calibration to filter out any noise.

3.2 System Boundaries

The System Under Test (SUT) is the Modular Temperature System (MTS). The block diagram of the SUT is shown in Figure 10. The MTS encompasses the Xilinx Virtex 5 ML507 Evaluation Platform, along with all the sub-components. Two important onboard components of the ML507 are the PowerPC 440 microprocessor and the Virtex 5 FPGA. On the FPGA, six identical digital temperature sensors are implemented from a custom VHDL module. The PowerPC 440 microprocessor executes the C++ code that controls the digital temperature sensors. The custom Digital Temperature Sensor is the Component Under Test (CUT) and the focus of this research.

This research limits the study of digital temperature sensors to implementation on FPGAs, since development is much quicker compared to fabrication, and FPGAs support the goal of a modular design. More specifically, this research uses only the Virtex 5 FPGA, although the results could most likely extend to other models.

3.3 System Services

The MTS provides one service to the user. On request, the system reports core temperature of the Virtex 5 over the UART serial interface for each of the sensors implemented on the Virtex 5. In this research, six temperature sensors are utilized,

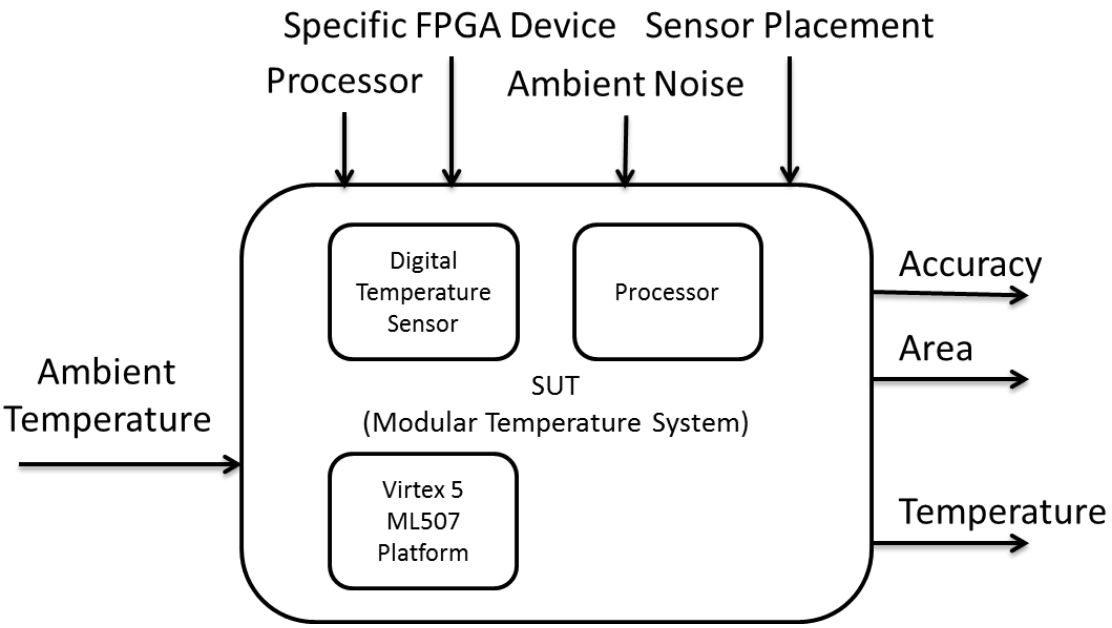


Figure 10. System Under Test block diagram.

and thus six temperatures are reported. The outcome of this service is ASCII text of the temperatures in Celsius. The service is active only after auto calibration. A failure outcome would be invalid/missing calibration data, which throws an error. Barring system malfunctions, no other failure outcomes are expected.

3.4 Workload

3.4.1 Ambient Temperature.

The only workload submitted to the system is the ambient temperature. The temperature affects the circuit delay of the FPGA which is used to infer temperature. Typically, the higher the temperature, the higher the delay, and thus the slower the device performs. Therefore, to measure the performance of the MTS, it is crucial that the temperature be controlled. The only parameters of this workload are the temperature range and increment level.

3.5 Performance Metrics

The following metrics are used to characterize the MTS, in order of importance to the research goals.

3.5.1 Digital Temperature Sensor Accuracy.

The accuracy metric supports a primary objective of this research. Accuracy is defined as the absolute difference between the System Monitor analog temperature sensor on the FPGA board and the temperature reported by MTS. The accuracy is measured after auto calibration at room temperature. Accuracy is measured at 9 temperature points, from 0 °C to 80 °C in 10 °C increments.

3.5.2 Digital Temperature Sensor Noise Resistance.

The digital temperature sensor noise resistance supports a primary objective of this research. Noise resistance is the ability of the sensor to retain accuracy while a main entity is concurrently running. The sensor is considered to be resistant to noise if there is no significant difference between the error of the sensor with and without the main entity running. A significant difference is defined as more than one standard deviation of error. The error for each digital temperature sensor is the difference between the System Monitor analog temperature sensor and the digital temperature sensor. The errors are measured after calibration at room temperature, unless otherwise stated.

3.5.3 Digital Temperature Sensor Precision.

The precision metric supports the secondary objective of this research. Precision is defined as the consistency of multiple readings of the same data, measured by the standard deviation of the temperature sensor readings at each temperature set point.

3.5.4 Digital Temperature Sensor Area.

Supporting the secondary objective of this research, percentage of total area utilized on the FPGA is measured via the resource utilization report from the Xilinx design tools, specifically the flip-flop, LUT, and BRAM resources.

3.6 System Parameters

3.6.1 Specific FPGA Device.

Several FPGAs of the same model are used in this research. While functionally equivalent, variations in the fabrication render each device unique at the physical submicron level. Consequently, physical characteristics such as delay are also unique to each device. Since the Digital Temperature Sensor correlates delay with temperature, the system is sensitive to a particular device. By varying the specific FPGA, the modularity of the sensor is tested. In other words, this parameter evaluates the ability of the sensor to calibrate appropriately to a particular device to ensure a high degree of accuracy on any Virtex 5 FPGA.

3.6.2 Ambient Noise.

The MTS is a secondary service for a primary system. However, the electric noise from the primary system can potentially affect the delay of the Digital Temperature Sensor, which can result in erroneous temperature readings and thus poor accuracy. To compare the accuracy in the presence of noise, a system without noise is compared to a system with additional circuitry designed to simulate an intense CPU load. Without noise is defined as only the circuitry of the MTS.

3.6.3 Microprocessor.

The Virtex 5 ML507 FPGA Platform provides two choices for a microprocessor a PowerPC 440 hardcore processor and a MicroBlaze softcore processor. The former is a fabricated processor on FPGA chip, while the latter is synthesized on the FPGA. The Digital Temperature Sensor accuracy may be dependent on the type of microprocessor used in the design. This research utilizes the hardcore PowerPC processor only.

3.6.4 Calibration Point.

The system uses one-point calibration for convenience. However, the error is expected to grow the further the temperature is from the one calibration point. Since the relationship between delay and temperature is not linear, the degree of error is dependant on the calibration temperature point. While an ideal temperature calibration point may yield the least overall error, room temperature is desirable since no external temperature chamber is required for calibration, allowing calibration to occur after deployment. Since this device may be used in extreme environments, room temperature may vary widely. Thus, different calibration temperature points are compared. The accuracy results from this parameter can then be used to determine whether recalibration is necessary, given accuracy and trust requirements of the mission.

3.7 Experimental Factors

The following discusses the factors and the levels chosen of the both the system parameters and the workload.

3.7.1 Specific FPGA Device.

Two different factor levels are used to vary the specific FPGA device (all of the same model). First, a single FPGA is used with six temperature sensors implemented on the device. The single FPGA is meant to test the intra-chip process variation. In other words, one digital temperature sensor is curve fitted from the System Monitor ADC and evaluated against the other five sensors after auto calibration.

The second factor level involves three FPGA boards with six temperature sensors implemented on each FPGA. This factor level is designed to test the inter process variation of the FPGAs. The additional two FPGA boards are all evaluated against the same digital temperature sensor originally curve fitted from the single FPGA board factor. The FPGA containing the curve fitted sensor is known as the Master FPGA. The FPGAs are chosen arbitrary and are not from the same fabrication batch, theoriectially representing worst case process variation.

3.7.2 Ambient Temperature.

The ambient temperature is varied to test the accuracy and latency of the MTS. The temperature is varied from 0 degrees Celsius to 80 degrees Celsius, in 10 degree increments, for a total of nine temperature values. This temperature range is chosen to encompass the anticipated operating range of this device once deployed in the field.

3.7.3 Ambient Noise.

Ambient noise is created by implementing a 512-bit RSA circuit on the Virtex 5 FPGA alongside the six temperature sensors. The 512-bit RSA circuit utilizes over 50% of the FPGA resources, providing a good workload to represent a highly computational circuit. This factor has two levels: with noise (RSA) and without noise (no additional circuitry).

3.7.4 Calibration Point.

The calibration point is varied to test the accuracy in different temperature environments when using auto calibration. Three calibration points are chosen to represent the expected range of sensor operation in even the most extreme environments. The three levels are 0 °C, 25 °C, and 50 °C.

3.8 Evaluation Technique

Direct measurement is the only practical evaluation technique since process variation is a major factor in this experiment, which is too difficult using simulation or an analytical approach. Furthermore, using actual hardware demonstrates the validity of this research more than a simulation. The following describes the experimental setup and the validation process.

The experimental setup is composed of three Virtex 5 ML507 FPGA Evaluation Platforms, a digitally-controlled temperature chamber, a digital thermometer, and a laptop computer. For a given experiment, one FPGA is placed inside the temperature chamber with connection lines (RS232, power, JTAG) routed through a penetration port to the laptop computer. The computer is able to download the FPGA design bitstream and control program execution while the FPGA is in an isolated environment. The computer is also connected to the temperature chamber via RS232 so the computer can control the temperature set point of the chamber. A picture of the setup is shown in Figure 11.

The first step of the experiment is to download the hardware bitstream (the hardware configuration) to the FPGA. Each FPGA is configured with the same design - six temperature sensors and a 512-bit RSA encryption circuit. The number of inverters in the delay line is set at 75, based on previous research [4] and empirical data. The baseline gain from which all digital temperature sensors are calibrated is set at

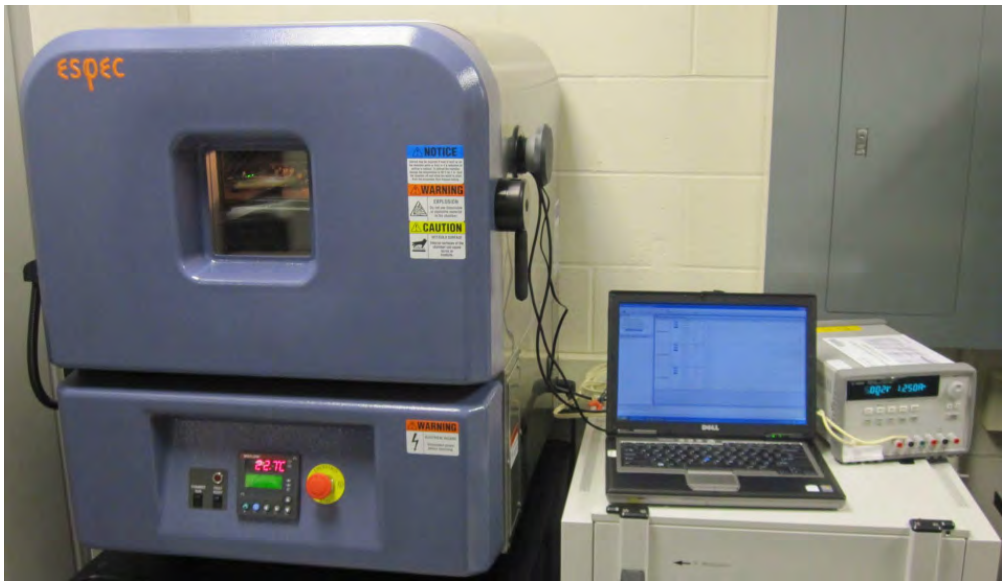


Figure 11. Experiment setup

8192 oscillations. The high gain and relatively short delay line ensures a very fine calibration resolution without a substantial increase in size or power consumption.

Each sensor is auto calibrated at room temperature (unless otherwise stated) using the Virtex onboard System Monitor ADC sensor as the one-point reference. While room temperature may not be the most accurate calibration temperature point, it is the most practical since no temperature chamber is required for operation outside the lab environment. The gain values of each sensor are now unique to account for the process variation among the sensors. The gain values are stored locally on the FPGA, and the device theoretically never needs calibration again. However, if the device will be used in a different temperature range, re-calibration is recommended to ensure the highest accuracy.

Once the device has gone through the auto calibration, the temperature reporting service is now active and the verification step begins. The temperature sensors are measured from 0 °C to 80 °C ambient temperature every 10 °C using a programmable temperature chamber. The FPGA is given five minutes at each point to reach thermal equilibrium prior to measurement, at which the core temperature is typically

10 °C to 15 °C higher than the ambient temperature. Each measurement consists of ten temperature readings. This process is repeated for each combination of selected experiments.

3.9 Experimental Design

For this research, a partial factorial experimental design is chosen. From previous research, such as [26] and [4], digital temperature sensors have very repeatable, stable responses. In addition, each factor tends to be independent and does not require iterating through all possibilities. This method allows for far fewer experiments, while maximizing the amount of information from analysis.

For the purposes of this research, one experiment consists of configuring the FPGA with a design, running the calibration program if required, and iterating through the nine temperature points. At each temperature point, ten readings are taken from the MTS. Thus, each experiment generates 90 readings for each sensor. Using six sensors generates 540 total readings.

For the single Master FPGA, one experiment is run both without any calibration and then using auto calibration. Next, three FPGA are run through the experiment to evaluate auto calibration with multiple FPGAs. The final experiment with auto calibration involves three temperature calibration points. Thus, auto calibration requires a total of eight experiments.

To evaluate noise resistance, a single FPGA is run with and without RSA active to justify the need for resistance. Two further experiments are performed to evaluate the two noise resistance methods attempted. Noise resistance therefore requires four experiments.

A combined total of 12 distinct experiments per design are required. In addition, other smaller prerequisite experiments may be required, such verifying the correctness

of the sensor, determining correct delay length, etc.

Variance is expected to be relatively low, since prior research has found digital temperature sensors to be very repeatable. Therefore, a 95% confidence interval is used. A failure indicates a lack of precision or accuracy. For thermal circuit protection, a false positive in detecting a large temperature change is more desirable than a false negative.

3.10 Methodology Summary

The goal of this research is to design and evaluate an improved digital temperature sensor implemented on a Virtex 5 FPGA ML507 Platform. The two major improvements are the auto calibration and noise resistance. The new design is evaluated by direct measurement using a digitally-controlled temperature chamber. Auto calibration is evaluated on a single FPGA and across multiple FPGAs. The calibration point is also varied as another factor. Noise resistance experiments vary the ambient noise. The digital temperature sensor, the component under test, is evaluated based on the accuracy, precision, and area.

IV. Design and Results

This chapter documents the digital temperature sensor design and results of the implementation. The system diagram is presented, along with details of the digital temperature sensor. Results include evaluating auto calibration both on one FPGA and across multiple FPGAs. Two methods for noise resistance are discussed. The effects of adding a main circuit (RSA) are studied and compared with the proposed noise resistant implementations. All results are evaluated using the metrics defined in Chapter 3, including accuracy and precision.

4.1 System Design

The proposed digital temperature sensor is implemented on an FPGA to facilitate quick development and deployment. The alternative of creating a custom chip requires fabrication, which is exponentially more expensive and time consuming than implementation onto an FPGA. The Xilinx Virtex 5 is chosen for this research because of its availability and popularity among researchers. The ML507 Evaluation board provides a platform to test the Virtex 5 and includes a Power PC, UART ports, RAM, JTAG programmer, etc. The system block diagram is shown in Figure 12.

For a given FPGA, six temperature sensors are implemented in two three-sensor arrays. Four control registers are used for each array - three registers for each of the sensor's output and one register to control all three sensors. The control register sends the START and RESET signals to the sensors, so all three are run simultaneously. The design details of the digital temperature sensor are presented below.

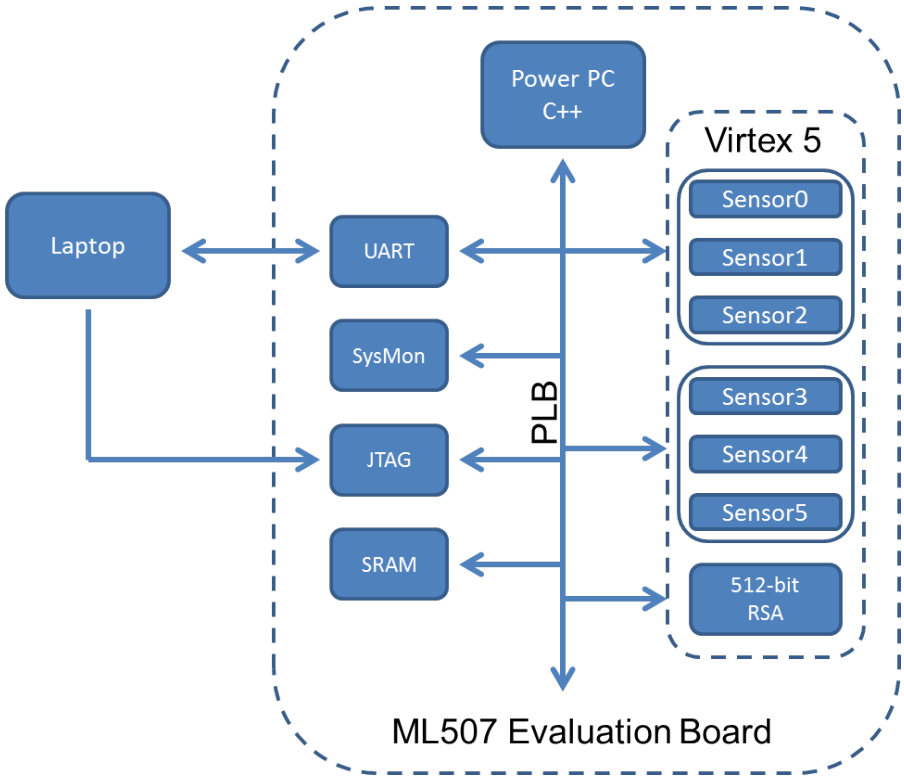


Figure 12. System block diagram

4.2 Digital Temperature Sensor Design

The proposed digital temperature sensor design is shown in Figure 13. The pulse based design measures the time for a ring oscillator to reach a variable number of circulations, rather than count the number of oscillations in a given time period. Assuming the system clock frequency is higher than the delay line oscillation frequency, the pulse based design is more precise since it eliminates potential residual delay not counted if the circulation has not completed.

The sensor is comprised of two main components - a delay generator and a time-to-digital converter. The delay generator uses a fixed ring oscillator and a counter to generate a circulation period sensitive to delay. The total circulation time is measured by creating a pulse: the START initiates the pulse and the counter terminates the pulse when the counter has reached the variable preset number of oscillations. The

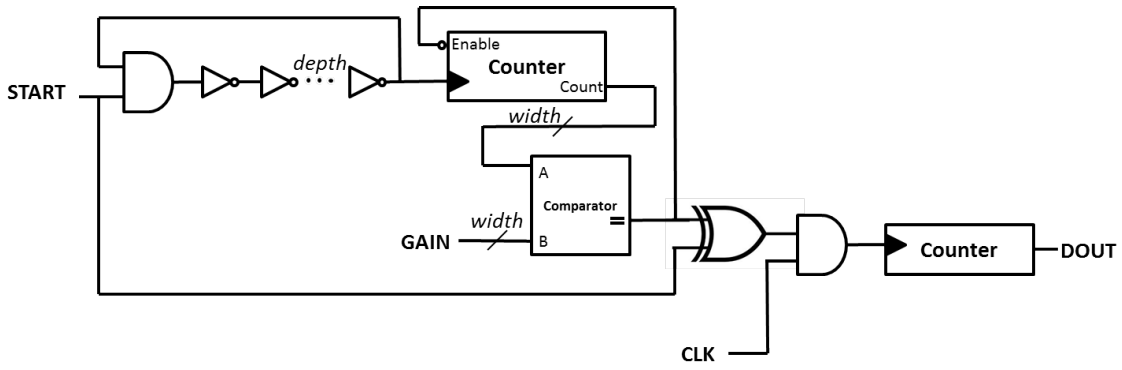


Figure 13. Proposed design of the digital temperature sensor

variable number of oscillations, known as the gain, allows for easy adjustment of the pulse width, an important aspect for calibration.

The time-to-digital converter digitally encodes the pulse width using the system clock as a reference. An AND gate continually increments a counter as long as the pulse is high, so that the time is effectively the number of clock cycles of the system.

The digital temperature sensor is built with a delay line length of 75 inverters, based on previous research and testing [4]. The delay line length is long enough to prevent self-heating, yet still use an incredibly small area of the FPGA, as discussed later in the chapter. The baseline gain from which all other sensors are calibrated is set at 8192 oscillations. The large gain allows for a sufficiently long delay to ensure a high degree of accuracy, as explained in Section 2.3.1. The high gain also provides more precise tuning for the calibration, since each oscillation accounts for a smaller percentage of the overall pulse width.

4.2.1 Auto Calibration.

An important feature of the sensor is auto calibration, which allows the device to be calibrated dynamically at its current temperature. Auto calibration, utilizing one-point calibration, offers several advantages over previous calibration methods discussed in Section 2.3.2. Full calibration, taking numerous measurements over the

range of expected use, is far too tedious for multiple devices and requires precision equipment to produce the desired temperatures. Two-point calibration is more practical. However, even two-point calibration still requires external equipment to achieve two significantly different temperature points. For thermal sensing applications, where many sensors are placed on a chip, each sensor is required to be independently calibrated. Thus, two-point calibration is not feasible for a digital temperature sensor.

One-point calibration allows for calibration at room temperature without external equipment. While one-point calibration is not as accurate as two-point calibration, the trade-off is significant cost and time savings, especially since precision and accuracy requirements may vary. For example, to detect the freezing attack referenced in Section 2.1, sensing a large change in temperature may be more important than the precision or accuracy of the exact temperature points.

One point calibration is made possible by the proposed sensor's variable gain input, which effectively adjusts the pulse width of each sensor. Since each temperature sensor will be unique at the physical level, the delay of each sensor on the device is also unique. The variable gain allows the calibration to normalize all temperature sensors to a reference device. The reference device is usually an analog sensor or another digital temperature sensor.

Auto calibration is the ability of the sensor to calibrate without user intervention. Since one-point calibration is possible at any given temperature, the user is not required to control temperature, unlike other methods of calibration. Other one-point calibration designs mentioned in Section 2.3.2 were not suitable for auto calibration. The sensor of [19] requires substantially more hardware than similar sensors, losing a key benefit of digital temperature sensors. The one-point calibration in [24] is implemented off chip and removed after initial calibration. Despite the size savings,

the sensor has lost the ability to recalibrate if the operating temperature changes significantly, increasing the error.

The following explains the calibration process. Propagation delay for an equal strength CMOS inverter is given by the following equation:

$$D = \frac{L}{W}\frac{C_L}{C_{ox}} * \frac{1}{\mu} * \frac{ln(3 - 4V_{th}/V_{dd})}{V_{dd}(1 - V_{th}/V_{dd})} \tag{2}$$

L = Gate Length, W = Gate Width

C_L = Load Capacitance

C_{ox} = Gate Oxide Capacitance

V_{th} = Threshold Voltage

V_{dd} = Supply Voltage

μ = Electron Mobility

Only two variables within this are affected by temperature: μ, the electron mobility, and V_{th}, the threshold voltage. It is estimated that the temperature dependence due to V_{th} is only a few percent of that due to μ and therefore negligible [19]. We assume, at a loss of accuracy, that μ varies linearly with temperature. Since the supply voltage V_{dd} is kept constant, the equation can be simplified to the following:

$$D = P * T * C \tag{3}$$

Here, P is the process variation, T is the temperature dependence, and C is the remaining constants. Since the length of the ring oscillator is fixed (but not the number of circulations), the delay represents one circulation of the ring oscillator.

The digital output $DOUT$ of the reference digital temperature sensor, known as the master sensor, is now:

$$Dout_M(T) = N_M * D_M = P_M * T * C * N_M \tag{4}$$

The term N_M is the gain (the number of oscillations required), chosen empirically or based on previous research. The master sensor is fitted to actual temperatures by multiple point calibration and least-squares regression. A second order polynomial model is utilized since it provides the best fit. Higher order models provide negligibly higher accuracy that is lost in calibration due to assumptions made earlier. This tedious portion is only required once to find the general correlation between delay and temperature for any sensor on any Virtex 5. The calibration temperature point T_C is chosen, usually room temperature, and the master $DOUT$ is recorded.

$$Dout_M(T_C) = N_M * D_M = P_M * T_C * C * N_M \tag{5}$$

For any other digital temperature sensor, one-point calibration is now possible. At the same calibration temperature, the $DOUT_I$ is recorded. The only unknown is the P_I, the process variation due to unique device fabrication.

$$Dout_I(T_C) = N_I * D_M = P_I * T_C * C * N_I \tag{6}$$

The process variation is compensated by adjusting the gain value for each individual device. At the calibration temperature, the gain is found by the difference in

the process, reflected by the difference in the $DOUT$ values.

$$N_I = \frac{N_M * Dout_M}{Dout_I} \tag{7}$$

After this one-point calibration, each device will ideally have the same $DOUT$ value for any given temperature, regardless of the physical differences and the unique delays. To recap, auto calibration assumes that the sensors all have the same slope and differ only by the y-intercept on the digital out vs temperature curve. A second order polynomial equation is fitted to one single sensor. Using a single temperature point, the unique y-intercept value is found that normalizes all the sensors to the general equation.

4.2.2 Noise Resistance.

Another key feature of the proposed digital temperature sensor is its resistance to digital component noise. The digital temperature sensor is meant to provide a critical auxiliary role alongside a main component operating within the same device. Implemented alone, the temperature sensor is clumsy and expensive at best. However, most previous research does not include a main computational activity in the implementation and experimentation. Because digital temperature sensors rely on the delay of integrated circuits, it is expected that additional circuitry running concurrently may effect this delay, and consequently the calibration and accuracy of the sensors. A more thorough investigation on the cause of noise is provide at the end of the chapter. While ignoring additional circuitry may provide a more accurate sensor, it is not realistic and does not support the original intent of the sensor. Thus, it is imperative that the sensor be immune to noise from other circuits. Two methods are proposed to filter out noise from the main activity: Noise Lock and Noise Calibration.

4.2.2.1 Noise Lock.

A lock is placed on the device while the digital temperature sensor is taking a sample, forcing the main circuit to remain idle during a temperature read, ensuring the sensor is free from noise. However, the obvious loss of computational time leads to slower devices, depending on the sensor sampling rate. It also may not be possible to lock a main circuit via an interrupt in the middle of a long main process.

4.2.2.2 Noise Calibration.

A more elegant solution is calibrating the sensor to account for the extra noise present. One-point calibration, as discussed earlier, is used twice - once with the main circuit in operation and once without, storing two gain vales for each sensor. The sensor is calibrated during the execution of the main circuit to filter out the noise generated. When sampling after calibration, the sensor checks whether the main activity is occurring and selects the correct calibration. Using this method, the main activity is not modified, and the circuit does not sacrifice speed or area. If the main circuit is modified, a quick recalibration is all that is required to maintain an accurate sensor.

4.3 Auto Calibration Results

The following section documents the results of the auto calibration experiments, both for a single FPGA and for multiple FPGAs. For experimentation, six digital temperature sensors are implemented on each FPGA. The single FPGA evaluates the inter-chip process variation, while the multiple FPGA experiment evaluates the intra-chip process variation. The single FPGA is the device used to generate the general correlation between a sensor's delay and temperature. This device is known as the Master FPGA.

4.3.1 Single FPGA.

Although all six temperature sensors are implemented on the same device, each still has their own process variation, and must be individually calibrated. To show the need for calibration, the measurement results for each sensor before calibration are shown in Figure 14. Here, the process variation is incorrectly assumed to be uniform for the entire device, and thus the gain of each sensor is fixed at 8192 oscillations. In other words, every sensor uses the equation of the Master Sensor relating delay to temperature.

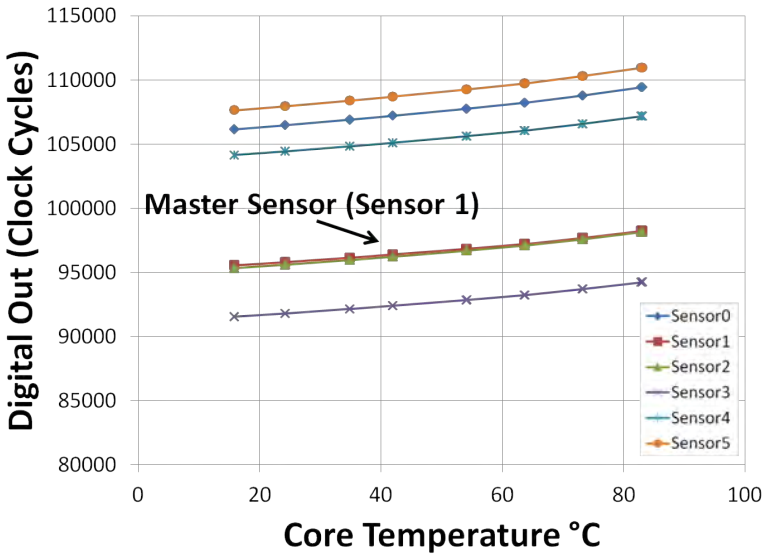


Figure 14. Digital temperature sensor response without calibration

The effect of device process variation is readily evident in Figure 14, resulting in a wide disparity of temperature readings. Thus, the need for individual calibration of each sensor is shown. Since the slope of each curve is roughly similar, only the y-intercept values separate these responses. Auto calibration adjusts the gain of each sensor, which correlates to the y-intercept values.

Auto calibration is run, calibrating each sensor simultaneously at room temperature using the onboard System Monitor ADC sensor as the one-point reference. Room

temperature is set at 25 °C. The same measurement is repeated, with results shown in Figure 15 on the same scale. The curves of each sensor are now normalized to the Master Sensor. After auto calibration, the unique gain of each sensor compensates for the device process variation and allows each sensor to give approximately the same digital out value for a given core temperature. A zoomed graphed is shown in Figure 16, highlighting the minuscule differences in slope among the sensors, causing error.

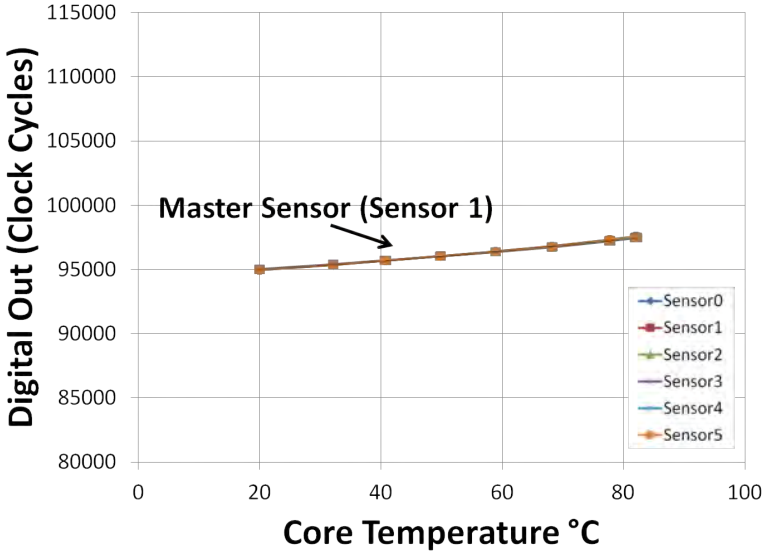


Figure 15. Digital temperature sensor response after auto calibration

4.3.1.1 Accuracy.

The average error of each sensor, using the System Monitor ADC as a reference, is shown in Figure 17, where the maximum error of all the sensors is about 4 °C. Taking the average of all the sensors at each temperature point yields a maximum error of 3 °C. The error here is due to the assumptions made earlier. Firstly, we assumed that μ varies linearly with temperature based on experimentally fitted data. As shown in Figure 17, the error increases the further the temperature point is from the calibration temperature. Another source of error is ignoring the effect of V_{th} on temperature. Although the effect is small, the process variation is not completely

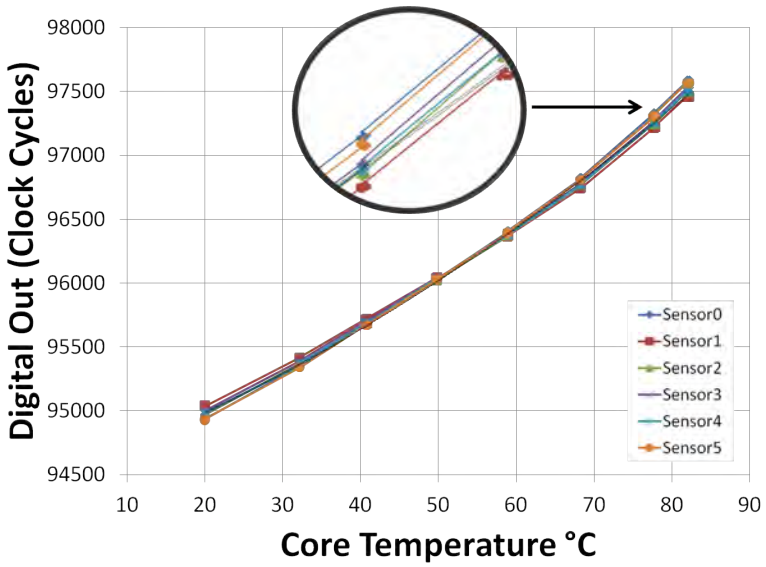


Figure 16. Digital temperature sensor response after auto calibration

removed, adding to the error. While these assumptions cause a decrease in accuracy, the simple equation allowing for one-point calibration translates to significant cost and time savings, as explained in Section 4.1.1.

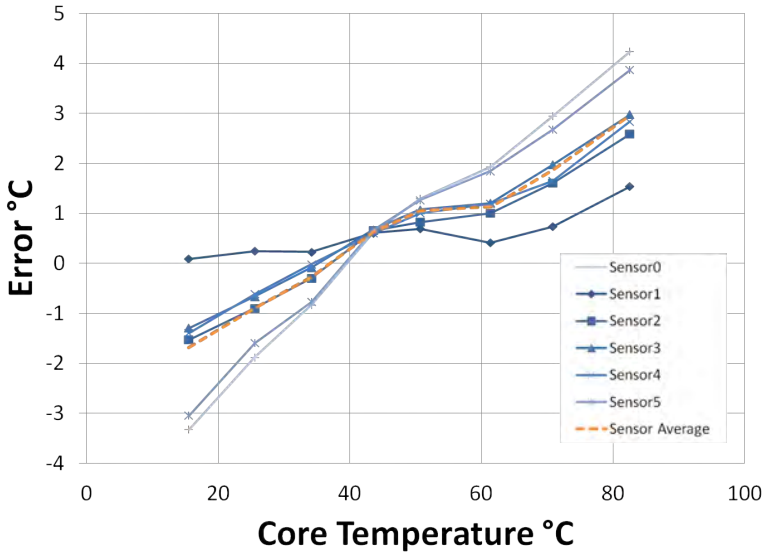


Figure 17. Digital temperature sensor response error vs System Monitor ADC on a single FPGA after auto calibration

4.3.1.2 Precision.

Precision ensures the digital temperature sensor is reliable even with one reading. The standard deviation of each sensor for each temperature point is shown in Figure 18. The precision is excellent, varying at most a quarter of a degree, consistent with previous research on the stability of temperature sensors. The precision seems to increase slightly at higher temperatures, but the change is insignificant.

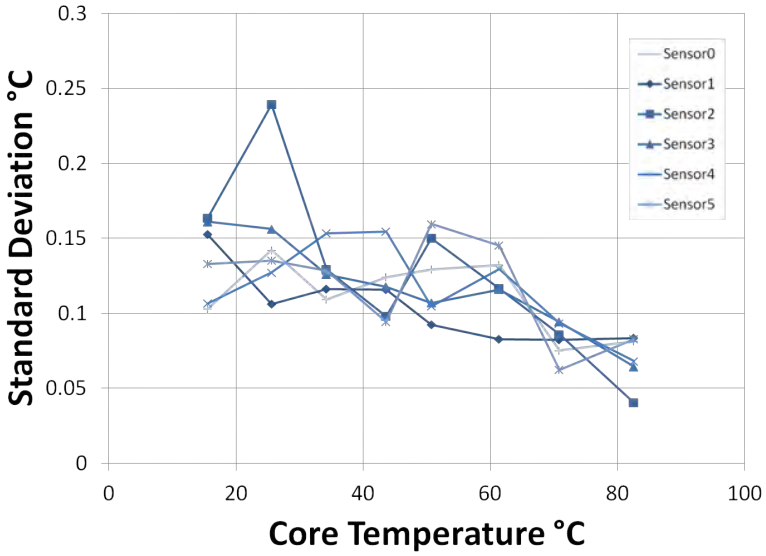


Figure 18. Digital temperature sensor response precision (standard deviation of 10 readings)

4.3.1.3 Area.

The secondary performance metric of area is measured using the Xilinx design tool PlanAhead. With the delay line length set at 75 inverters, an array of three digital temperature sensors uses just 291 registers and 455 LUTs. The Virtex 5 XC5VFX70T has a total of 44800 registers and LUTS, rendering utilization at around 1%. Decreasing the delay line length reduces the utilization even further, but increases the chance of self-heating. Self-heating can cause the temperature sensor to add heat to the area it is measuring, negating the calibration and generating significant error.

4.3.2 Multiple FPGAs.

Auto calibration is now evaluated across multiple FPGAs. The inter-chip process variation is expected to be greater than the intra-chip process variation evaluated on a single FPGA in the previous section. All sensors on a single FPGA have obviously gone through the exact same fabrication process. As such, the PMOS and NMOS strength of the inverters is much more similar than that of an inverter fabriated in a separate process on another chip. Thus, the single FPGA is expected to have less process variation than across two different FPGAs. Three FPGAs are calibrated at room temperature using their respective onboard System Monitor ADC sensors, yet using the correlation coefficients obtained from the Master FPGA (FPGA 0)as the reference for all sensors. The results of the sensors are shown in Figure 19.

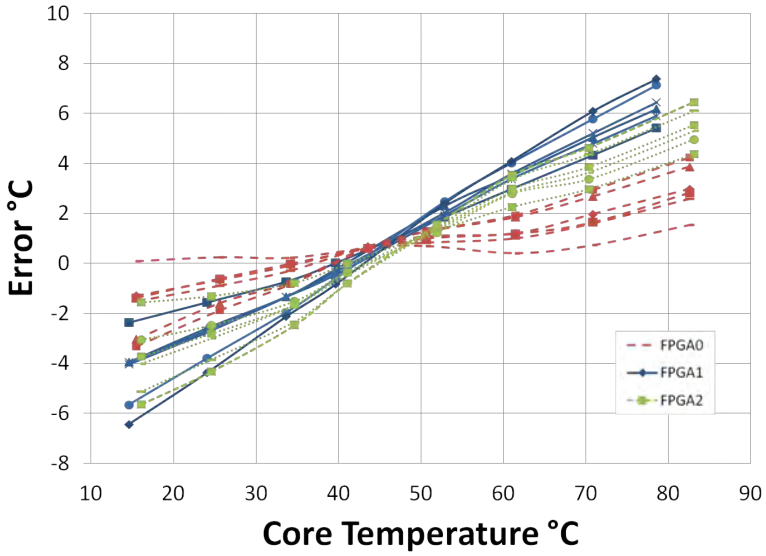


Figure 19. Digital temperature sensor response error vs System Monitor ADC across 3 FPGAs after auto calibration

4.3.2.1 Accuracy.

The average error of the ten readings of each sensor is shown in Figure 19. As expected, sensors from the FPGA used to derive the master curve (on the master

Table 1. Max error of averaging sensors at each temperature point

	Max Avg Error (± 20 °C)	Max Avg Error (± 30 °C)
FPGA0	1.26	3.0
FPGA1	3.59	6.4
FPGA2	2.96	5.45

FPGA 0) have the least error. The increased inter-chip process variation produces a greater error among sensors from the remaining FPGAs, due to the assumptions discussed previously. The max error for any one sensor is about 7 °C. Averaging among all the sensors on a given chip brings the error down even further. Table 1 presents the average for all the sensors on each FPGA in a practical format. If the sensor is operating within 20 °C from its calibration point, the error at under 4 °C might be acceptable. However, if the operating temperature expands to 30 °C or more from its calibration point, accuracy drop to a potentially unacceptable 6 °C max error and a recalibration might be required.

4.3.2.2 Precision.

Precision across three FPGA boards is measured by the standard deviation of the ten temperature readings at each temperature point. Results are shown in Figure 20. The precision is not unlike the precision of sensors on a single FPGA. Therefore, process variation, even across multiple FPGAs, does not significantly affect the precision.

4.3.3 Multiple Calibration Points.

Up until this point, the calibration temperature has been fixed at room temperature, which for out purposes is 25 °C. Although this value represents the most likely temperature for calibration outside the lab environment, the device may be used in

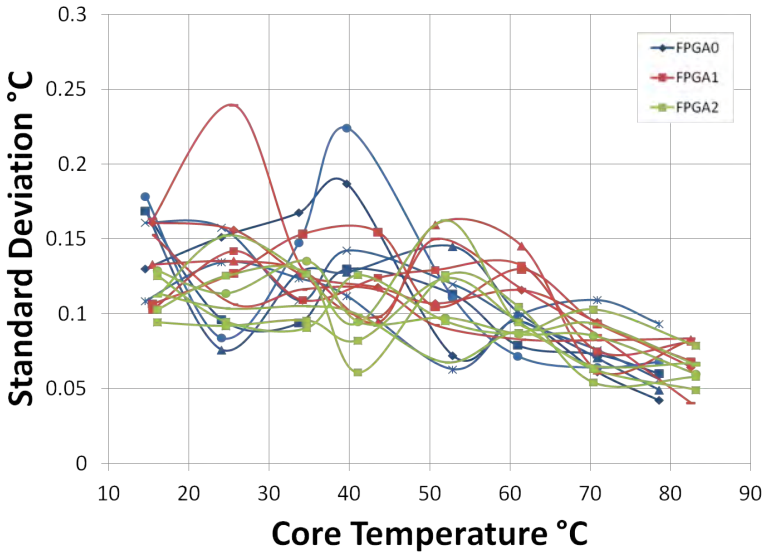


Figure 20. Digital temperature sensor response precision across 3 FPGAs

extreme temperatures (either hot or cold) and must retain its accuracy. As seen previously, the error of the sensor increases the further the operating temperature is from the calibration temperature. To minimize error, the device should be recalibrated near the expected operating temperature. The error at three different calibration points is shown in Figure 21.

As expected, the average error increases the further the temperature point is from the calibration point. In order to keep the error at a reasonable level across the entire temperature spectrum, recalibration is necessary. Specifically, the need for recalibration is evident when the core temperature is $\pm 30°C$ from the calibration temperature, when the average error may exceed 5 °C. Considering that this experiment is done on the Master FPGA, the additional error from increased process variation on other FPGA may yield an unacceptable error. While recalibration can increases the accuracy, it also introduces a vulnerability for sensors used in defense application. Since the recalibration uses the System Monitor ADC as a reference, any exploitation of the analog sensor could compromise the digital temperature sensors during recalibration - the reason the digital temperature sensor is utilized in the first place. Thus,

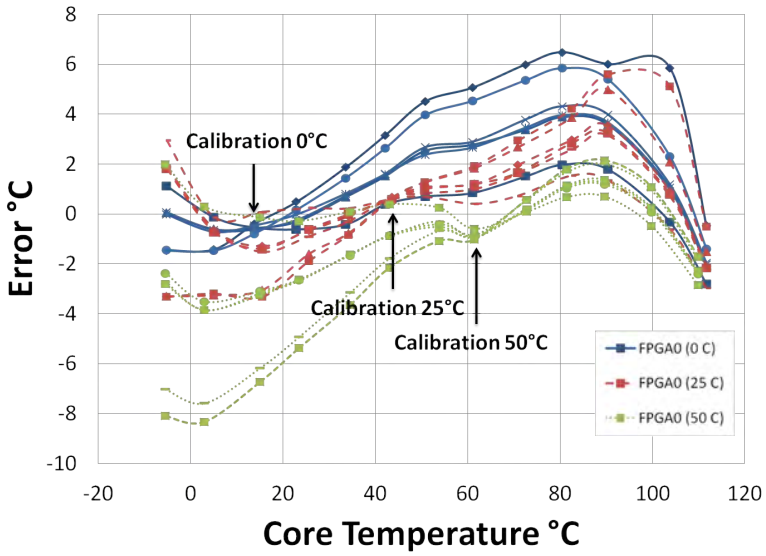


Figure 21. Digital temperature sensor response at 3 calibration temperature points on a single FPGA

recalibration should be used sparingly, depending on the accuracy requirements and the trust of the reference sensor.

4.4 Noise Resistance Results

Here, results of the noise resistance are presented. A 512-bit RSA encryption circuit is implemented on the same FPGA as six digital temperature sensors. To evaluate the impact of the RSA circuit and show the need for noise resistance, the six temperature sensors are measured with the RSA circuit disabled vs concurrently encrypting during the temperature readings, shown in Figure 22.

Clearly, RSA impacts the accuracy of the sensor. The higher digital out values with RSA running indicate the sensors required more time to complete the oscillations and thus were slower. The two proposed methods to filter out the effects of RSA, namely Noise Lock and Noise Calibration, are now evaluated.

First, results from implementing the noise lock are shown in Figure 23. As expected, the Noise Lock mitigates the enormous sensor error caused by RSA. Since the

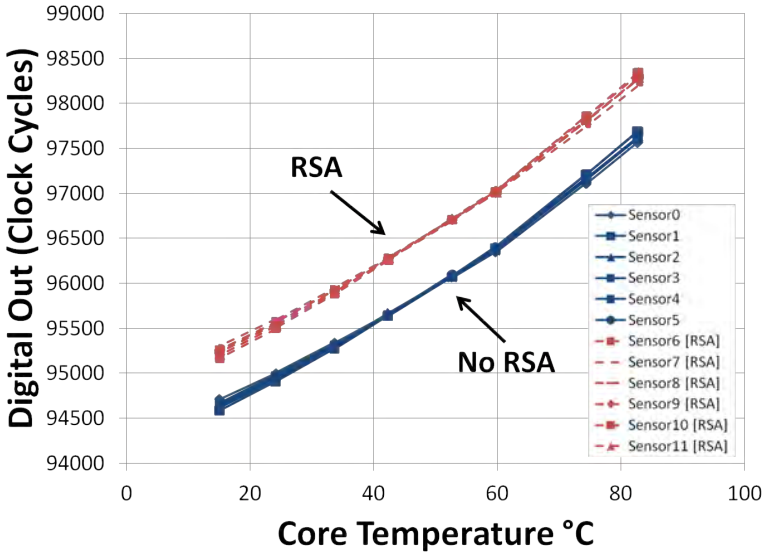


Figure 22. Digital temperature sensor error with 512-bit RSA computing

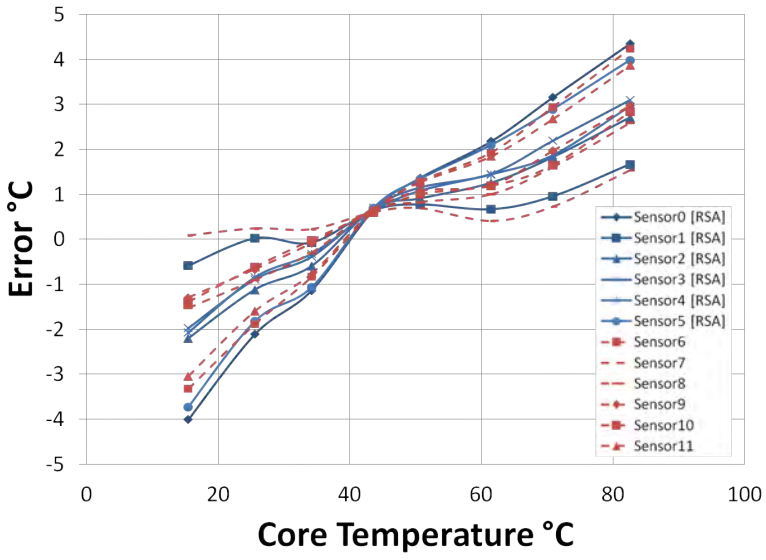


Figure 23. Digital temperature sensor response with 512-bit RSA computing using Noise Lock

Noise Lock effectively separates the two processes, they run independently just as if the temperature sensor was running without RSA. The obvious caveat is that sensor readings cause delay in the RSA circuit. To allow RSA to run concurrently alongside the digital temperature sensors, the other proposed method of Noise Calibration is evaluated, with results shown in Figure 24. It appears that Noise Calibration is able to correct the offset from the RSA noise.

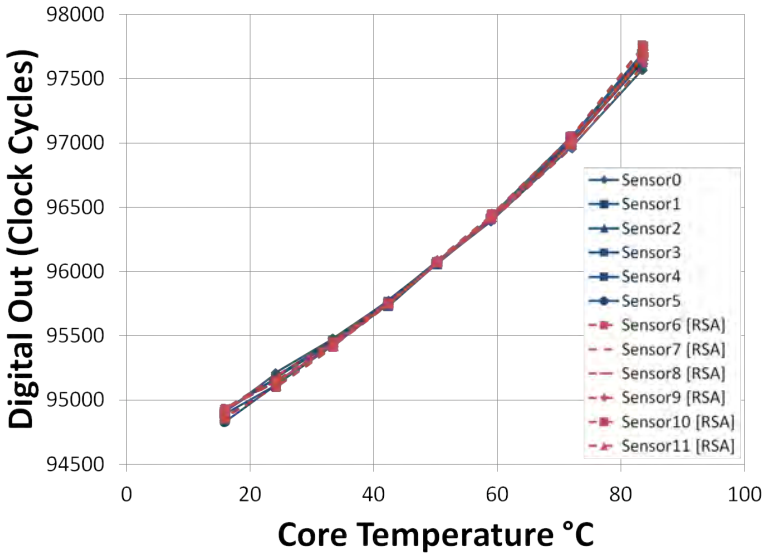


Figure 24. Digital temperature sensor response with 512-bit RSA computing after Noise Calibration

Looking at the error in Figure 25, the sensor performs no worse in the presence of noise after Noise Calibration compared with calibration without noise. Thus, the digital temperature sensor is able to run alongside a main circuit without a substantial loss of accuracy, so long as a separate calibration is run simultaneously with the main circuit to account for the additional noise. The error is also approximately the same as the Nock Lock method, except without the performance penalty.

Standard error bars are added to the previous graph to quantitatively check the difference between the two curves, assuming a normal distribution. For clarity, only three sensors are shown. The only failure is for sensor 0 (sensor 6 w/RSA), and only

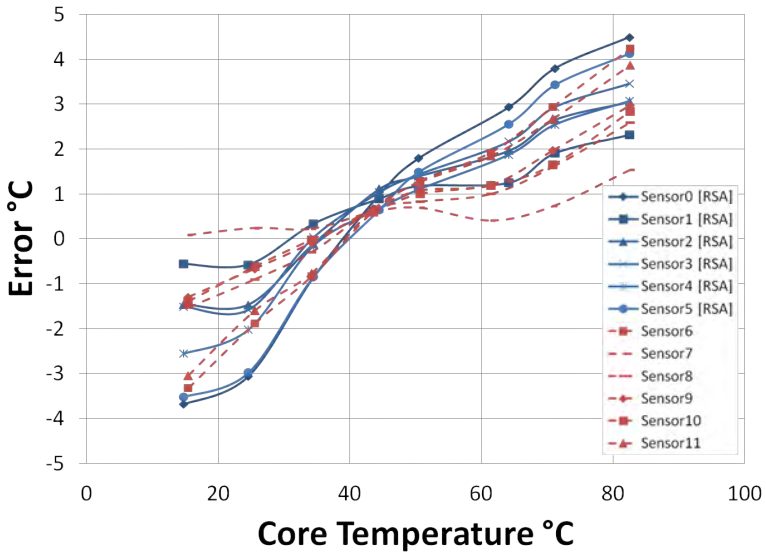


Figure 25. Digital temperature sensor error with 512-bit RSA computing after Noise Calibration

at temperatures distant from the calibration point. However, the error is so low for this sensor in either case, it can be safely ignored.

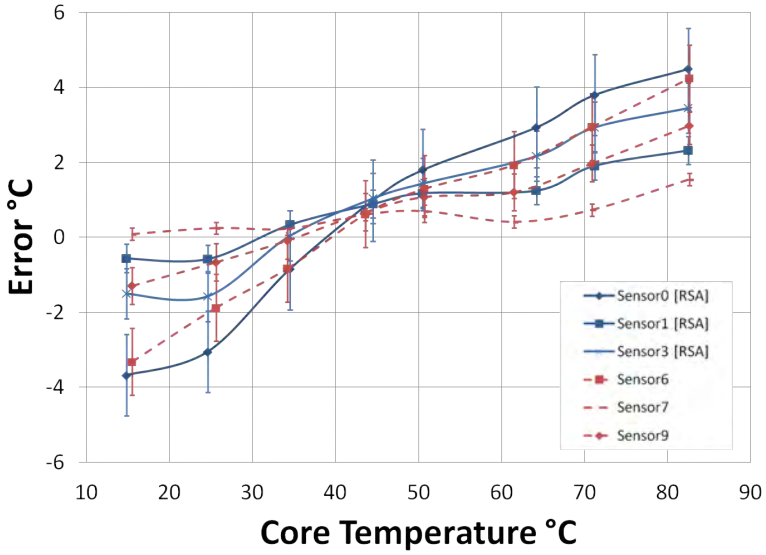


Figure 26. Digital temperature sensor error with 512-bit RSA computing after noise calibration

It is difficult to point to the exact source of noise from the additional RSA circuit. Since the circuit and sensors are implemented on an FPGA, the specific details of

the design are left to the Xilinx synthesizer. Two major sources of internal noise in integrated circuits are: noise coupled from a common resistive path or noise that is capacitively coupled from another signal path [27]. The result is a drop in voltage, dependant on the number of gates changing states simultaneously. A drop in voltage equates to an increase in delay. In the case of the large 512-bit RSA circuit, the change in voltage is significant. Normally this change in voltage isn't a problem with digital circuits since the circuit will functionally operate the same but with a slight speed penalty. Yet, because a digital temperature sensor is highly dependant on this speed, any voltage drop will affect accuracy.

Another probable cause for noise is the load capacitance. Since the digital temperature sensors are implemented on the same FPGA chip as the 512-bit RSA circuit, it is highly likely that they share circuitry from routing, buses, etc., which will increase the capacitance at the output nodes of the logic gates and contribute to the overall delay of the circuit [27]. Figure 27 summarizes the impact of both capacitance and voltage on the delay of a circuit.

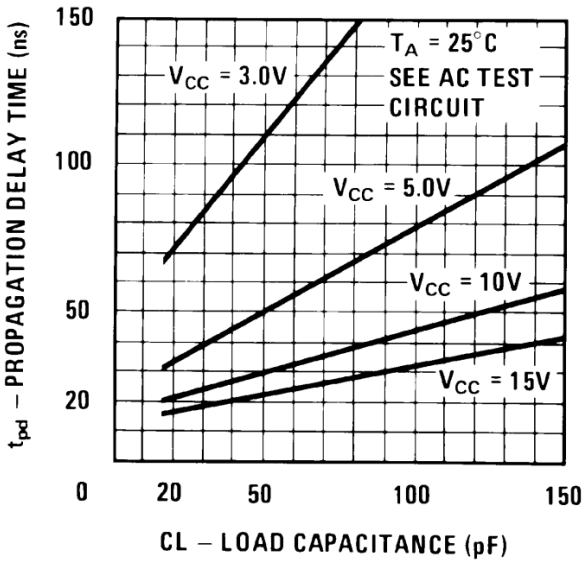


Figure 27. CMOS inverter propagation delay vs load capacitance for varying voltages [8]

Clearly, both voltage and load capacitance are known to affect the delay of integrated circuits. As seen in the graph, lower voltages magnify the effect of load capacitance on delay. Noise calibration would in effect be calibrating out the change in voltage or capacitance. Initially, voltage was assumed to be kept constant, which means any change in voltage requires a recalibration. Regardless of the specific reason, the recalibration with the inclusion of noise allows the sensor to operate with no worse accuracy than calibration without the noise.

V. Conclusions

5.1 Research Goals

The purpose of this research was to design and evaluate an improved digital temperature sensor for circuit protection. The two significant improvements studied were the addition of auto calibration and noise resistance. The goal of auto calibration was to develop a quick, one-point calibration method that can operate on any FPGA of the same model, saving time and money, as well as permitting operation in the field. The other primary goal was to evaluate the sensor in the presence of noise from a main circuit and develop methods to mitigate negative effects.

5.2 Conclusions

These goals were met by developing a noise resistant digital temperature sensor with auto calibration. The pulse based design using a delay generator with a time-to-digital converter is more precise than counting delay loops in a given time. The variable preset number of oscillations allows for adjustment of the pulse width. One point calibration then adjusts the pulse of each sensor to account for the unique process variation of each sensor. To define a reference pulse width, a sensor designated as the Master sensor was fitted against the analog diode sensor on the Master FPGA. Noise resistance was achieved by running the auto calibration concurrently with the main entity, thus calibrating out the noise. The sensor chooses the appropriate gain depending if the main circuit is active.

Evaluation of the auto calibration accuracy confirms the modularity of the sensor. On the Master FPGA within ± 30 °C of the calibration temperature, the maximum error was only 3.0 °C when averaging the sensor response at each temperature point. Among three FPGA, where the fabrication variation is assumed to be higher, the

same maximum average error increased to 6.4 °C. Decreasing the temperature span to ± 20 °C brings that number down to 3.6 °C. Thus, accuracy decreases slightly when using the sensor on an arbitrary FPGA of the same model. Changing the calibration temperature had a negligible effect on the accuracy. The conclusion is that the sensor can operate with a tolerable accuracy on any Virtex 5 FPGA at any calibration temperature between 0 °and 50 °C. Recalibration can reduce these errors even further.

Studying the effects of running a main circuit alongside the sensor showed a substantial error due to increase in delay at similar temperatures. The proposed solution calibrates out the difference by running the auto calibration concurrently with the main circuit. Results of the noise calibration showed no worse accuracy when compared with calibration without noise. The conclusion is that the sensor can operate with a main circuit as designed without compromising performance.

5.3 Contributions

This research produced an advanced digital temperature sensor suitable for thermal circuit protection. By discreetly monitoring the core temperature of digital devices, the sensor is able to react to drastic changes in temperature due to freezing or heating attacks. To protect the circuit, the sensor can trigger the erasure of the sensitive data, such as encryption keys, or shutdown the device to prevent damage. Auto calibration ensures a modular design that can easily be implemented on any Virtex 5 and achieve reasonable accuracy. Recalibration allows the sensor to adapt to changing temperature environments in the field. In addition, auto calibration using one temperature point allows numerous sensors to be deployed simultaneously and instantly be calibrated and ready for use, saving substantial time and costs over sensors requiring individual calibration. The sensor is also able to operate alongside a

main component embedded on the same chip by calibrating out the noise otherwise adversely affecting the sensor. Thus, the sensor is able to accurately protect a circuit in close proximity.

5.4 Recommended Future Work

This research could be extended in several areas. First, the sensor could be implemented and tested on different models of FPGAs, as well as different FPGA manufacturers. The sensor could also be tested alongside different main entities, such as other encryption circuits or even multiple entities. More research could also be done on the cause of the effects from the encryption circuit, which may lead to other methods of filtering out the noise.

Appendix A. Digital Temperature Sensor VHDL code

```
----------------------------------------------------------------------------------
-- Company: AFIT
-- Engineers: Lt Brandon Brown
-- Create Date:    14:31:54 07/16/2010
-- Design Name:
-- Module Name:    sensor - Structural
-- Project Name:
-- Target Devices:
-- Tool versions:
-- Description:
--
-- Dependencies:
--
-- Revision:
-- Revision 0.01 - File Created
-- Additional Comments:
--
----------------------------------------------------------------------------------
library IEEE;
use IEEE.STD_LOGIC_1164.ALL;
use IEEE.STD_LOGIC_ARITH.ALL;
use IEEE.STD_LOGIC_UNSIGNED.ALL;



entity sensor is
    Generic (width : positive := 13; depth : natural := 20);
    Port (      clk : in STD_LOGIC;
```

```
                en    : in STD_LOGIC;
                reset : in STD_LOGIC;
                gain    : in STD_LOGIC_VECTOR (width-1 downto 0);
                count_out : out  STD_LOGIC_VECTOR (width-1 downto 0));
end sensor;

architecture Structural of sensor is

    component counter32 is
    Generic (width : positive);
        Port (  clk     : in STD_LOGIC;
                reset   : in STD_LOGIC;
                en      : in STD_LOGIC;
                sum     : out  STD_LOGIC_VECTOR (width-1 downto 0)
              );
    end component;

    component RingOscillator is
    Generic (N : positive);
        Port (  EN      : in  STD_LOGIC;
                osc_out : out  STD_LOGIC);
    end component;

    component andGate2 is
        Port (  in1     : in  STD_LOGIC;
                in2     : in  STD_LOGIC;
                out1    : out  STD_LOGIC);
    end component;
```

```
    component xorGate2 is
        Port (  in1     : in  STD_LOGIC;
                in2     : in  STD_LOGIC;
                out1    : out  STD_LOGIC);
    end component;

    component comparator is
    Generic (width : positive);
        Port (  A       : in  STD_LOGIC_VECTOR (width-1 downto 0);
                B       : in  STD_LOGIC_VECTOR (width-1 downto 0);
                less    : out  STD_LOGIC;
                equal   : out  STD_LOGIC;
                greater : out  STD_LOGIC);
    end component;

    signal cycles_counted : std_logic_vector (width-1 downto 0);
    signal osc_output, compare_equal, xor_out, and_out : std_logic;


begin

    RO1: RingOscillator generic map (N => depth) -- N gives N + 1 inverters in delay line
            port map(EN => en, osc_out => osc_output);

    delay_counter:  counter32 generic map (width => width)
            port map(clk => osc_output, reset => reset, en => compare_equal,
            sum => cycles_counted);
```

```
    compare: comparator generic map (width => width)
            port map(A => cycles_counted, B => gain, equal => compare_equal);

    xor_gate: xorGate2 port map(in1 => compare_equal, in2 => en, out1 => xor_out);

    and_gate: andGate2 port map(in1 => xor_out, in2 => clk, out1 => and_out);

    output_counter:  counter32 generic map (width => width)
            port map(clk => and_out, reset => reset, en => '0', sum => count_out);

end Structural;
```

Bibliography

[1] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Cal, A. J. Feldman, and E. W. Felten, "Least we remember: Cold boot attacks on encryption keys," in *In USENIX Security Symposium*, 2008.

[2] S. Lopez-Buedo, J. Garrido, and E. Boemo, "Thermal testing on reconfigurable computers," *IEEE Design & Test of Computers*, vol. 17, no. 1, pp. 84–91, 2000.

[3] P. Chen, M.-C. Shie, Z.-Y. Zheng, Z.-F. Zheng, and C.-Y. Chu, "A fully digital time-domain smart temperature sensor realized with 140 FPGA logic elements," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 54, no. 12, pp. 2661–2668, 2007.

[4] J. J. L. Franco, E. Boemo, E. Castillo, and L. Parrilla, "Ring oscillators as thermal sensors in FPGAs: Experiments in low voltage," in *Proc. VI Southern Programmable Logic Conference (SPL)*, pp. 133–137, 2010.

[5] D. Ha, K. Woo, S. Meninger, T. Xanthopoulos, E. Crain, and D. Ham, "Time-domain cmos temperature sensors with dual delay-locked loops for microprocessor thermal monitoring," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, no. 99, pp. 1–12, 2011. Early Access.

[6] P. Chen, S.-C. Chen, Y.-S. Shen, and Y.-J. Peng, "All-digital time-domain smart temperature sensor with an inter-batch inaccuracy of -0.7 c - +0.6c after one-point calibration," *IEEE Transactions on Circuits and Systems I: Regular Papers*, no. 99, 2010. Early Access.

[7] R. Mukherjee, S. Mondal, and S. O. Memik, "Thermal sensor allocation and placement for reconfigurable systems," in *Proc. IEEE/ACM International Conference Computer-Aided Design (ICCAD)*, pp. 437–442, 2006.

[8] Fairchild Semiconductor, *CMOS Oscillators*, application note 118 ed., October 1974.

[9] D. Goodin, "Apple secuirty is struggling," *www.theregister.co.uk/2009/06/09/apple_security_suggestions*, June 2009.

[10] J. Cole, "Protecting america's intellectual property assets," *http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202491664461&Protecting_Americas_intellectual_property_-assets&slreturn=1&hbxlogin=1*, April 2011.

[11] A. Bakker and J. H. Huijsing, "Micropower CMOS temperature sensor with digital output," *IEEE Journal of Solid-State Circuits*, vol. 31, no. 7, pp. 933–937, 1996.

[12] A. Bakker, "CMOS smart temperature sensors - an overview," in *Proc. IEEE Sensors*, vol. 2, pp. 1423–1427, 2002.

[13] P. Dadvar and K. Skadron, "Potential thermal security risks," in *Proc. IEEE Twenty First Annual IEEE Semiconductor Thermal Measurement and Management Symp*, pp. 229–234, 2005.

[14] J. Kong, J. K. John, E.-Y. Chung, S. W. Chung, and J. Hu, "On the thermal attack in instruction caches," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 2, pp. 217–223, 2010.

[15] S. Skorobogatov, "Local heating attacks on flash memory devices," in *Proc. IEEE Int. Workshop Hardware-Oriented Security and Trust (HOST)*, pp. 1–6, 2009.

[16] P. Chen, M.-C. Shie, Z.-F. Zheng, C.-Y. Chu, M.-H. Chiang, and Z.-Y. Zheng, "A fully digital low cost time domain smart temperature sensor with extremely tiny size," in *Proc. IEEE Asian Solid-State Circuits Conf. ASSCC 2006*, pp. 147–153, 2006.

[17] S. A. Bota, M. Rosales, J. L. Rossello, and J. Segura, "Smart temperature sensor for thermal testing of cell-based ICs," in *Proc. Design, Automation and Test in Europe*, pp. 464–465, 2005.

[18] C.-C. Chung and C.-R. Yang, "An all-digital smart temperature sensor with auto-calibration in 65nm cmos technology," in *Proc. IEEE Int Circuits and Systems (ISCAS) Symp*, pp. 4089–4092, 2010.

[19] K. Woo, S. Meninger, T. Xanthopoulos, E. Crain, D. Ha, and D. Ham, "Dual-DLL-based CMOS all-digital temperature sensor for microprocessor thermal monitoring," in *Proc. IEEE Int. Solid-State Circuits Conf. - Digest of Technical Papers (ISSCC)*, pp. 68–69, 2009.

[20] C.-C. Chung and C.-R. Yang, "An autocalibrated all-digital temperature sensor for on-chip thermal monitoring," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 58, no. 2, pp. 105–109, 2011.

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

[22] P. Chen, K.-M. Wang, Y.-H. Peng, Y.-S. Wang, and C.-C. Chen, "A time-domain SAR smart temperature sensor with inaccuracy for on-chip monitoring," in *Proc. 34th European Solid-State Circuits Conference (ESSCIRC)*, pp. 70–73, 2008.

[23] P. Chen, T.-K. Chen, Y.-S. Wang, and C.-C. Chen, "A time-domain sub-micro watt temperature sensor with digital set-point programming," *IEEE Sensors Journal*, vol. 9, no. 12, pp. 1639–1646, 2009.

[24] P. Chen, S.-C. Chen, Y.-S. Shen, and Y.-J. Peng, "All-digital time-domain smart temperature sensor with an inter-batch inaccuracy of-0.7 to 0.6 after one-point calibration," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 58, no. 5, pp. 913–920, 2011.

[25] S. O. Memik, R. Mukherjee, M. Ni, and J. Long, "Optimizing thermal sensor allocation for microprocessors," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 27, no. 3, pp. 516–527, 2008.

[26] E. Boemo and S. Lopez-Buedo, "Thermal verification on FPGAs," in *Proc. 23rd NORCHIP Conf*, pp. 48–53, 2005.

[27] R. L. Geiger, *VLSI Design Techniques for Analog and Digital Circuits*. McGraw-Hill Publishing Company, 1990.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
22–03–2012	Master's Thesis	Aug 2010 — Mar 2012

4. TITLE AND SUBTITLE

AN FPGA NOISE RESISTANT DIGITAL TEMPERATURE SENSOR WITH AUTO CALIBRATION

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Brown, Brandon A., 2d Lt.

5d. PROJECT NUMBER

12G292O

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GCE/ENG/12-02

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Dr. Robert L. Herklotz
Program Manager - Information Operations and Security Air Force Office of Scientific Research (AFOSR/RSL)
875 N. Randolph Street, Suite 325, Room 3113
Arlington, VA 22203-1768
703-696-6565 robert.herklotz@afosr.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

AFOSR/RSL

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In recent years, thermal sensing in digital devices has become increasingly important. From a security perspective, new thermal based attacks have revealed vulnerabilities in digital devices. Traditional temperature sensors using analog-to-digital converters consume significant power and are not conducive to rapid development. As a result, there has been an escalating demand for low cost, low power digital temperature sensors that can be seamlessly integrated onto digital devices. This research seeks to create a modular Field Programmable Gate Array digital temperature sensor with auto one-point calibration to eliminate the excessive costs and time associated with calibrating existing digital temperature sensors. In addition, to support the auxiliary protection role, the sensor is evaluated alongside a RSA circuit implemented on the same chip, with methods developed to mitigate noise and power fluctuations introduced by the main circuit. The result is a digital temperature sensor resistant to noise and suitable for quick mass deployment in digital devices.

15. SUBJECT TERMS

digital temperature sensor, thermal management, thermal attack, smart temperature sensor, ring oscillator, time to digital, auto calibration, noise resistance, one point, calibration

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Maj Todd R. Andel USAF (ENG)
U	U	U	UU	71	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636, x4901; todd.andel@afit.edu