Programmable Signal Acquisition and Calibration of Temperature Sensors for Detection of Power Dissipation on Chips

Alexis Chen, YSP Student, *Lexington High School*
Brendan O'Riordan, YSP Student, *Boston Latin School*
Thomas Gourousis, Electrical and Computer Engineering, *Northeastern University*
Minghan Liu, Electrical and Computer Engineering, *Northeastern University*
Yunfan Gao, Electrical and Computer Engineering, *Northeastern University*
Prof. Marvin Onabajo, Electrical and Computer Engineering, *Northeastern University*

Abstract

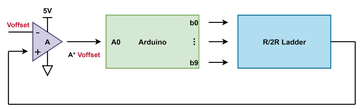
Motivation: The main goal of our project is to insure hardware security by preventing integrated circuits from being tampered with malicious circuits.

Personal Objectives: To get hands-on laboratory experience working with hardware and software to help solve a problem with real-world applications.

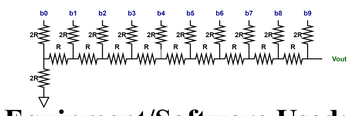
Results: We developed a system level approach to calibrate amplifier offsets. We sense the amplifier voltage, compared it to a reference voltage, and developed Arduino code that controls the output of a DAC converter in order to adjust the input voltage of the amplifier.

Experimental Methods

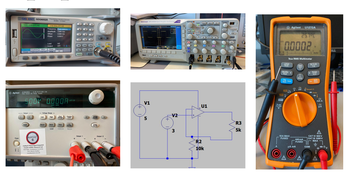
System Level Overview:



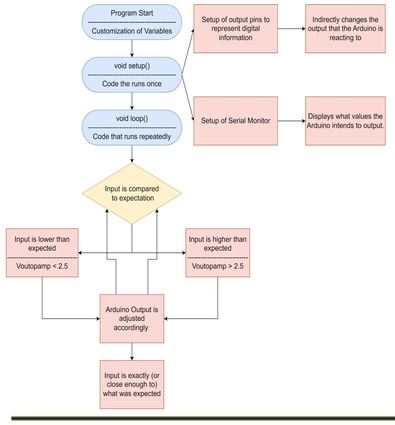
R/2R Ladder:



Equipment/Software Used:



Algorithm Flowchart:



Op-Amp:

An essential part of our design for detecting trojans are amplifiers, which are fundamental building blocks in analog electronics.

However, random mismatches during manufacturing and packing lead to an offset in the relationship between input and output signals.

We want to detect offset and minimize it.

Digital-to-Analog Converter:

Unfortunately, the Arduino cannot output analog signals.

To gain access to a broader range of Arduino output voltages, we created a DAC (digital to analog converter).

Background

Modern Circuit design and manufacturing involves too many tasks at different companies around the world to prevent Integrated Circuits (ICs) from being tampered with.

Malicious circuits installed on integrated circuits are known as Trojan circuits.

They are inserted into empty spaces, and they are too small to detect visually or by weight.

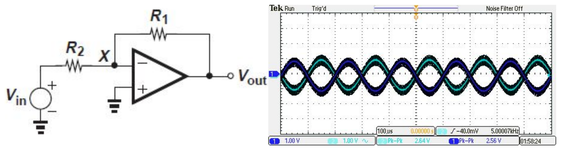
Our project focuses on using temperature sensors to detect the presence of Trojan circuits to improve the security of Internet of Things (IoT) devices.

Results

Proving that the Op-Amp Works:

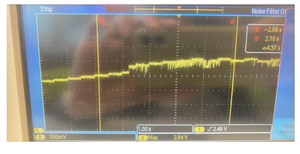
Op-Amps are often used in closed-loop configuration in order to prevent saturation.

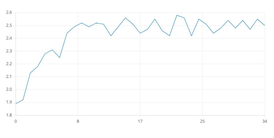
Using specifically the inverting op-amp, we are able to control amplifier gain using external components (resistors), and actually invert a signal.



Op - Amp placed in feedback loop with R2 = R1 = 10 KΩ
Measurement results from inverting configuration:

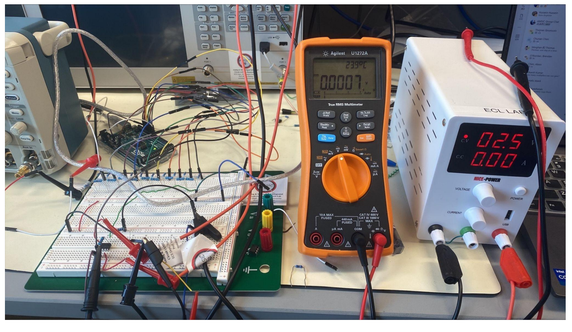
- Input signal : 5 KHz and 2.56 Vpp
- Output signal : 5 KHZ and 2.64 Vpp
- If Vin = 0 then we can measure amplifier offset





Proving that the DAC Works:

- Digital bits input - analog voltage output
- Output voltage only in discrete steps
- 3 bit DAC - 2^3 = 8 possible combinations
- Each step VLSB = Vref / 2^3 = 5 /8 = 0.625V
- Arduino code cycles through 8 possible combinations 000 - 111
- Oscilloscope used for measuring output
- Output Voltages : [0.625 - 4.375] V
- Final output voltage Vref - VLSB ~= 4.375 V



Conclusion and Future Steps

The code developed in this project will be modified to work directly on the chip that is being measured. The circuit will be adjusted to be closer to ideal for greater precision.

Our algorithm was written to be customizable, but when it gets used more and more, additional variables will be added to give testers more precise control over its performance.

References

John O'Malley, 2011. *Schaum's Outline of Basic Circuit. Analysis Revised Second Edition*. McGraw-Hill Education.

Razavi, B., 2021. *Fundamentals of Microelectronics*. John Wiley & Sons.

M. Yan, H. Wei and M. Onabajo, *"On-Chip Thermal Profiling to Detect Malicious Activity: System-Level Concepts and Design of Key Building Blocks,"* in IEEE Trans. Very Large-Scale Integr. (VLSI) Syst, vol. 29, no. 3, pp. 530-543, March 2021.

T. Gourousis, Z. Zhang, M. Yan, M. Zhang, A. Mittal, A. Shrivastava, F. Restuccia, Y. Fei, and M. Onabajo, *"Identification of Stealthy Hardware Trojans through On-Chip Temperature Sensing and an Autoencoder-Based Machine Learning Algorithm,"* to appear in Proc. IEEE Intl. Midwest Symp. Circuits Syst. (MWSCAS), Aug. 2023. [Accepted]

Acknowledgements

AMSIC Research Laboratory
Marvin Onabajo, *Associate Professor*
Thomas Gourousis, *Ph. D. Candidate*
Minghan Liu, *Ph. D. Candidate*
Yunfan Gao, *Ph. D. Candidate*

Center for STEM Education
Claire Duggan, *Executive Director*
Jennifer Love, *Associate Director*
Claire Stipp & Yassine Souabny, *YSP Coordinators*
Nicolas Fuchs, *Project Implementation Coordinator*
Mary Howley. *Administrative Officer*

Young Scholars Program at Northeastern University
Claire Duggan, Program Director

This material is based upon work supported by the National Science Foundation under grant no. 2146754 and is supported in part by funds from OUSD R&E, NIST, and industry partners as specified in the Resilient & Intelligent NextG Systems (RINGS) program.