# Title

Design and Security of Analog and Mixed-Signal Circuits with Innovations in Temperature Sensing for Power/Thermal Management, Trojan Detection in Analog Filters, and Optimization for Programmable Current Mirrors.

# Abstract

This work presents a novel CMOS-based temperature sensor aiming to improve on-chip power/ thermal management by monitoring potential hotspot formation across different locations on a semiconductor die. The sensor is designed with two correlated output voltages, which embeds temperature information within the ratio of the two voltage outputs, allowing for self-referencing capabilities. This unique design enables direct temperature-to-digital conversion without the need for a separate reference for the converter, resulting in compactness and high accuracy for power and thermal management applications. The sensor demonstrates low sensitivity to variations in bias current caused by temperature fluctuations across the die. This low sensitivity allows for compactness, while the self-referencing capability ensures great accuracy of the digital conversion. Both dual-temperature and single-temperature calibration methods are introduced to achieve optimal performance of the novel temperature sensor, providing an economical solution while maintaining precision.

Experimental validation using devices fabricated in 0.18μm and 0.5μm CMOS processes showed a sample 3σ measurement error after a two temperature calibration of less than ±1ºC across a wide temperature range from -10ºC to 100ºC under constant current bias and a ±5% bias current variation over the same temperature range. Even with a single temperature calibration, requirements are met for power/thermal management purposes.

The research also identifies hardware security vulnerabilities related to hardware Trojans in widely used filter structures. It highlights the susceptibility of prevalent filter architectures to an unexpected, nondestructive, stationary, nonlinear oscillatory mode. This mode poses challenges in detection during the design, verification, and testing phases, potentially disrupting filter functionality until a power reset is initiated. The work presented in this dissertation delves into the primary nonlinearities responsible for this behavior and uncovers security vulnerabilities in common filter designs due to hardware Trojans. By examining continuous time filters such as the KHN filter, the Tow-Thomas filter structures, and switched-capacitor filters, the research demonstrates the crucial relationship between passive component values and the nonlinear parameters of amplifiers in either fostering or preventing this undesired oscillatory mode. Experimental results from discrete component Tow-Thomas and KHN filters illustrate the susceptibility of the filter to this self-oscillatory mode, which could be exploited for Trojan operations within the filter architecture.

Finally, a digitally programmable current mirror design is introduced to optimize resource utilization, reduce costs, and simplify the complexity associated with unit cells.