Design and implementation of a multi-modal sensor with on-chip security

Ava Hedayatipour
ahedaya1@vols.utk.edu

Follow this and additional works at: https://trace.tennessee.edu/utk_graddiss

Recommended Citation
https://trace.tennessee.edu/utk_graddiss/6873

This Dissertation is brought to you for free and open access by the Graduate School at TRACE: Tennessee Research and Creative Exchange. It has been accepted for inclusion in Doctoral Dissertations by an authorized administrator of TRACE: Tennessee Research and Creative Exchange. For more information, please contact trace@utk.edu.
To the Graduate Council:

I am submitting herewith a dissertation written by Ava Hedayatipour entitled "Design and implementation of a multi-modal sensor with on-chip security." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Electrical Engineering.

Nicole McFarlane, Major Professor

We have read this dissertation and recommend its acceptance:

Benjamin J. Blalock, Garrett S. Rose, Steven A. Ripp

Accepted for the Council:

Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)
Design and implementation of a multi-modal sensor with on-chip security

A Dissertation Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Ava Hedayatipour

August 2020
Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. 1816703 and by the U.S. Department of Energy, Office of Science, Office of Basic Energy Sciences under Award Number DE-SC0017414.

I would like to express my gratitude to Dr. Nicole McFarlane, whom without her contagious passion and guidance this work would have not been possible. More than an advisor during my Ph.D. program she has been a role model. I am thankful to Dr. Benjamin Blalock and Dr. Garrett Rose for their contributions and encouragements. I appreciate them and Dr. Steven Ripp serving as my committee members and I thank them for their valuable suggestions.

I will forever be thankful to my colleagues Farnaz Foroughian, Sharam Hatefi Hesari, Aminul Haghue, Kendra Anderson and my other lab-mates in MK540 and MK538 for all the good times. I'll never forget the many wonderful lunches and hallway talks. I especially thank Shaghayegh Aslanzadeh, my sister away from home. I am also grateful for all my friends in ISA-UTK and Systers organization.

I sincerely thank my partner Nima Hoseinzadeh for more than a decade of friendship and always being by my side through this roller coaster of a ride. Thanks to my family back in Iran and friends from IUST now scattered around the world, that motivated me to keep going forward. I am extremely lucky to have wonderful friends (Pegah, Parinaz, Golnaz, Saeed, Hosein and many more) keeping me sane through this journey. My mother, sister and father have been the best support system all my life. My hard-working parents have sacrificed a lot to show me life, as I know it know.
Abstract

With the advancement of technology, wearable devices for fitness tracking, patient monitoring, diagnosis, and disease prevention are finding ways to be woven into modern world reality. CMOS sensors are known to be compact, with low power consumption, making them an inseparable part of wireless medical applications and Internet of Things (IoT). Digital/semi-digital output, by the translation of transmitting data into the frequency domain, takes advantages of both the analog and digital world. However, one of the most critical measures of communication, security, is ignored and not considered for fabrication of an integrated chip. With the advancement of Moore’s law and the possibility of having a higher number of transistors and more complex circuits, the feasibility of having on-chip security measures is drawing more attention. One of the fundamental means of secure communication is real-time encryption. Encryption/ciphering occurs when we encode a signal or data, and prevents unauthorized parties from reading or understanding this information. Encryption is the process of transmitting sensitive data securely and with privacy. This measure of security is essential since in biomedical devices, the attacker/hacker can endanger users of IoT or wearable sensors (e.g. attacks at implanted biosensors can cause fatal harm to the user). This work develops 1) A low power and compact multi-modal sensor that can measure temperature and impedance with a quasi-digital output and 2) a low power on-chip signal cipher for real-time data transfer.

First, an impedance sensor is designed using a current comparator for measuring the resistance portion of the impedance and voltage comparators for the capacitance measurement. The sensor eliminates the need for the switches and the sink and source current sources, common in impedance sensors. This array-able, low power sensor delivers the output in terms of frequency, which is suitable for wireless transmission. The other
sensor is a sub-\(\mu\)W temperature sensor that uses a sub-threshold proportional to absolute temperature voltage generator, a comparator, and a 3-transistor voltage reference to convert temperature to frequency.

Second, an encryption/decryption block is designed using time scaling chaotic shift keying to have security on-chip and immunity to well-known attacks such as the return map attack. The goal of the system is to provide relatively low power consumption. Synchronization of the two chaotic systems to have the same state is the primary key in chaotic encryption. In this work, a Lorenz based chaotic shift keying (CSK) system is used and a differential Lorenz chaotic block is then implemented on the same chip as the multi-modal impedance and temperature sensor. This ciphering block encryptes the output pulse before transmission. After transmission, the signal is received by another CSK system which deciphers the message by synchronization of two systems.
# Table of Contents

1 Introduction
   1.1 Research Goals .................................................. 5
   1.2 Dissertation Overview .......................................... 6

2 Literature Review
   2.1 Impedance Sensor ................................................ 9
       2.1.1 Impedance Sensing Circuits .............................. 11
   2.2 Temperature Sensor ............................................. 16
       2.2.1 Temperature Sensing Circuits ............................ 18
   2.3 Chaotic Ciphering ............................................... 21
       2.3.1 Chaotic Ciphering Circuits ............................... 23
   2.4 Conclusion ...................................................... 30

3 Impedance Sensor
   3.1 Design ............................................................ 31
   3.2 Simulation and Experimental Results .............................
       3.2.1 Resistance Sensor .......................................... 35
       3.2.2 Capacitance Sensor ........................................ 38
       3.2.3 Human Experiments ........................................ 42
   3.3 Conclusion ...................................................... 49

4 Temperature Sensor
   4.1 Design ............................................................ 51
List of Tables

3.1 Transistor sizing for different blocks. ........................................ 34
3.2 Comparison table with state of art impedance measurement. ............ 43
3.3 Human experiments done 5 times in a day every 3 hours showing measured resistance, capacitance and standard deviation. ......................... 50
4.1 Transistor sizes for 130nm 8rf temperature sensor chip ...................... 54
4.2 Transistor sizes for 180nm temperature sensor chip ......................... 55
4.3 Comparison table with state of art temperature Sensor. .................... 62
5.1 Comparison table with state of art chaotic communication. ............... 88
List of Figures

1.1 The global market for wearable technology has increased from just over US $10 billion in 2016 to US $51.6 billion in 2021. .................................................. 2

1.2 Proposed design showing temperature and impedance sensor along with real-time encryption decryption system .......................... 6

2.1 Three main topologies for cell impedance sensing [31]. ....................... 12

2.2 Illustration of impedance-to-frequency topology with alternate current sink and source [12]. ................................................................. 13

2.3 Lock-in approach in impedance sensing, voltage-mode lock-in amplifier sweeps the frequencies of the sinusoidal signal applied to the electrodes and measures the imaginary and real part of the output signal [39]. ............... 14

2.4 Cell impedance measurement using silicon cochlea [46]. .................... 16

2.5 Current controlled voltage sources bipolar junction transistor as a temperature sensor. ................................................................. 18

2.6 Reference clock generating a temperature based delay. ...................... 20

2.7 Temperature sensing using a current controlled oscillator [65]. .......... 20

2.8 Temperature sensing using weak inversion MOS devices [68]. ........... 21

2.9 Folded temperature sensor [69]. ...................................................... 21

2.10 Illustration of the Chaotic Cryptosystem for communications [92]. .... 27

2.11 Block diagram of oscillator unit [93]. ........................................... 27

2.12 Chaotic oscillator architecture proposed in [87]. ............................... 28

2.13 Circuit board photo of oscillator unit to see the size and number of components for a discrete chaotic ciphering transmitter [94]. ....... 29
2.14 Circuit board photo of oscillator with no passive elements [96].

3.1 Impedance to frequency conversion circuit.

3.2 Current comparator characterization using DC sweep. (a) Current comparator having 6 µA on one input and a sweeping 4 to 8 µA on the other, showing and output change of GND to VDD on 6 µA. (b) Positive input is swept from 4 to 8 µA, while the negative input is stepped from 4 to 8 µA in 1 µA increments (c) Gain of the current comparator.

3.3 Current comparator simulation output for a changing sinusoidal input compared to a constant DC current input for 2 different reference current.

3.4 The transient response for experimental impedance measurement for 2 different comparison.

3.5 Different system output pulse width for difference impedance showing linear duty-cycle with decrease in impedance.

3.6 SR-latch output showing high output when set signal is high, and low output when reset is high.

3.7 System output frequency for different impedance.

3.8 Voltage comparator characterization using DC sweep. (a) Positive input is swept from 0 to 1 V while the negative input is stepped from 0-1 V in 100 mV increments. (b) Gain of the current comparator.

3.9 System output frequency for different capacitance.

3.10 The transient response for 100 nF experimental impedance measurement.

3.11 Impedance to frequency converter layout.

3.12 RC simultaneous measurement showing (a) a change in resistance measurement with 3 capacitance values, 10 nF, 47 nF, and 100 nF and (b) a change in capacitance measurement with 3 resistance values, 1 kΩ, 5 kΩ, and 10 kΩ.

3.13 Bare conductive paint is used to (a) draw electrodes on filter paper, (b) the electrodes are then cut, the wire put on the paint, and (c) put on skin with the system using medical tape to measure the impedance.

3.14 Impedance measurement system.
3.15 The thoracic impedance measurement system. .................................. 46
3.16 Hand gesture recognition system. .................................................. 47
3.17 FM receiver setup with Arduino. .................................................... 48
3.18 Hand gesture recognition results showing the impedance of sign language letter A-D. The impedance is measured in ratio to relax status in (a) heat map (b) line plot. .................................................. 49
4.1 Frequency based temperature sensing system with a single comparator. ... 52
4.2 Final frequency based temperature sensing system using weak inversion MOSFETs. ............................................................ 53
4.3 Output frequency variation for temperature change of 0 °C to 50 °C in steps of 0.5 °C for 180 nm temperature sensor. ........................................ 56
4.4 Temperature sensor output at 3 different temperatures, 0 °C (11.82 kHz), 25 °C (27.72 KHz) and 50 °C (50.23kHz) for 180 nm temperature sensor. .. 57
4.5 Frequency output signal at 0, 25, and 50 °C for 130nm technology temperature sensor. ............................................................ 58
4.6 Distribution of frequency output over the temperature range 0 °C to 50 ° for 130 nm technology temperature sensor. ........................................ 58
4.7 Output voltage as a function of temperature for 25 °C to 150 °C for chip fabricated in 130 nm CMOS technology. ........................................ 59
4.8 Experimental verification of the comparator for chip fabricated in 130 nm technology. ............................................................ 59
4.9 Experimental setup for temperature to time sensor using a temperature chamber. ............................................................ 60
4.10 Experimental measurements of temperature to time sensor using a temperature chamber for chip fabricated in 130 nm technology. ............ 60
4.11 Noise spectral density at 10 kHz over the operational temperature range for chip fabricated in 130 nm technology. ........................................ 61
5.1 Chaotic shift keying return map determined using $x$. ......................... 68
5.2 Return time map calculated using TS-CSK encryption. ......................... 69
5.3 CSK transmitter system block diagram. ........................................ 73
5.4 CSK receiver system block diagram. ........................................ 73
5.5 TS-CSK system transmitter. .................................................. 74
5.6 TS-CSK system receiver. ...................................................... 75
5.7 (a) TS-CSK circuit schematic (b) Modulator circuit schematic. .... 75
5.8 Signal extraction circuit. ....................................................... 76
5.9 Temperature sensing system translates VPTAT to frequency. The signal is then encoded using a chaotic transmitter and decoded with the receiver. The transmitter and receiver may be connected using wires or wireless. .... 77
5.10 Experimental setup of temperature sensor implemented in a CMOS 130nm BiCMOS process, and transmitter and receiver system with discrete components on PCB. ......................................................... 78
5.11 Experimental measurements. (a) $V_{PPTAT}$ corresponding to 50°C temperature, sent to a transmitter to be encoded. (b) Voltage is encoded and sent as a secure signal. (c) Matlab simulink used to decode the secure sensor in simulation. (d) The experimental decoded temperature signal in the receiver. (e) Experimental temperature signal which is decoded in the receiver goes through optimization algorithms. Local peak detection to remove noise (solid line) and thresholding (dashed line) is used to optimize the signal. .... 79
5.12 Integrator circuit. ............................................................... 80
5.13 Multiplier circuit. ............................................................. 81
5.14 Multi-modal sensors output is chosen by a simple analog multiplexer and then fed to a chaotic transmitter. ......................................................... 81
5.15 CMOS-based MUX device built using two transmission gates. ........ 82
5.16 The encryption chip fabricated in 130 nm BiCMOS technology. .... 82
5.17 Integrator in 130 nm BiCMOS input versus output transient response. . 83
5.18 Differential input/output Gilbert cell implemented in 130 nm BiCMOS transient response. .............................................................. 83
5.19 Single ended chaotic system showing no oscillation. .................. 84
5.20 Fully differential on-time ciphering system. ............................ 84
5.21 Simulation results of yz output showing chaotic behaviour of the circuit in 180 nm. .......................................................... 85

5.22 Experimental result of the coded and decoded signal by the ciphering transmitter and receiver implemented in 180 nm. (a) The temperature signal input to the the transmitter, (b) the transmitter input and the receiver output, and (c) the decoded signal at the output of the receiver. .................. 86

5.23 Implementation of the transmitter and receiver on a prototype board. .... 87

1  Layout of impedance sensing system chip fabricated in 180 nm technology. . 112
2  Layout of temperature sensing system chip fabricated in 130 nm technology. 113
3  Layout of temperature sensing system chip fabricated in 180 nm technology. 114
4  Layout of amplifier and multiplexer fabricated in 180 nm technology. ....... 114
5  Layout of integrator fabricated in 180 nm technology. ......................... 115
6  Layout of integrator fabricated in 130 nm technology. ......................... 116
7  Layout of Gilbert Cell fabricated in 180 nm technology. ....................... 117
8  Layout of Gilbert Cell fabricated in 130 nm technology. ....................... 118
9  Layout of security system fabricated in 180 nm technology. .................. 119
Chapter 1

Introduction

Technology plays a rapidly growing role in our lives. Day by day, we become increasingly dependent on technology and less willing to separate ourselves from it. Technology’s tendency to become faster and smaller has given rise to a new generation of wearable technology, from fitness trackers and the SmartWatch to Smart Glasses and Smart Contact Lens. The last two decades have seen an unprecedented increase in wearable technology usage. It is expected that the global market for wearable technology which was US $750 million in 2012 will increase to over US $50 billion by 2022. In 2019, around 60 million people used a wearable/portable device in the United States, and increase of 9.2% over 2018, Fig. 1.1 [1].

One of the primary reasons for the popularity of wearable technology is the global increase in the aging population. In the coming years, the percentage of older aged adults will increase twofold, posing numerous health challenges. Aged populations, living alone, require long-term monitoring for a better independent life. The aging populations demand good care quality, preferably in a remote manner, to prevent disturbing their comfort. The element of price is also an important parameter in this scheme. In this context, wireless wearable sensor networks for medical use, once a topic of science fiction nature, are becoming a necessity. According to eMarketer’s latest wearable forecast, use of wearables is growing the fastest in middle aged Americans, 55 and older, mainly due to their enhanced health features [2].

Apart from the prominent wearable applications, many more wearable applications are under research and test and device development is a hot topic of much interdisciplinary research. These designed systems are becoming more and more mature in recent years and are
The global market for wearable technology has increased from just over US $10 billion in 2016 to US $51.6 billion in 2021.

moving from research fields to commercial devices. Using wearable devices provides a more convenient way to extract accurate measurements of vital signals, along with physical and physiologic parameters. Wearable applications have various applications in different areas of health care and clinical practices, such as prevention (activity tracking, eating behavior and calorie intake tracking, stress monitoring), diagnosis (early detection, different symptoms tracking), and disease management (monitoring of drug intake and drug reminders). Though no person can pinpoint the specific applications of the next generation wearables that are going to be hit, people have plenty of ideas.

Sweat-sensing glasses with a printable electrochemical sensor array implemented on disposable nose-piece pads is among the new generation of wearables. This chemical-sensing smart glasses would collect and analyze sweat. To go further, there is the possibility of using slightly invasive—but painless—wearables in the near future, such as flexible stickers full of micro-needle sensor arrays that can track chemical changes just under the skin. An example application detects the presence of an enzyme using a bio-marker, particularly within skin moles for the quick monitoring of skin melanoma [3]. Though availability of more accurate, sensitive, and stable devices is critical, there have been parallel efforts in integrating wearable devices with smart processing. Artificial intelligence which relies on modern techniques of machine learning/pattern recognition and data aggregation is the frequent algorithm of choice implemented. Having connected devices with the internet (wearables, vehicles, sensing nodes, household supplies) enables continuous data acquisition. More importantly,
with the progress of systems-on-chip real-time information processing is added to each device. Recent implementations of devices such as motion trackers, heart-rate tracker, and intelligent watches do more than monitoring movements and heart rate and showing the data. Adding processing units helps these devices to analyze personal data and provide algorithms to study our daily life and behaviors. Nowadays, in the age of data, users can be more cognizant of different effects of their behaviors, like sleeping patterns and exercises on their health, through the use of algorithms for pattern recognition. As an example, you can see how exercise affects sleep patterns, or if sleeping earlier and the activity range of the next day has any relation. Data can also be integrated from different sources like stress level, current or past mood, and food logs to further improve the algorithm development and introduce new parameters in these algorithms. Having new parameters can predict later actions and habits, and its effect on health by refining the summary of past practices, actions, and experience. Sensors can have more applications than just on-body, and as wearable devices, they can be integrated on other surfaces and be used along with sensors in buildings and vehicles. Although there have been numerous implementations of wireless devices, there are still significant challenges to be solved regarding wearables. Reliability, power consumption, data transfer, security, materials, size, and flexibility are among these issues.

**Reliability:** One of the limitations of wearable devices is the assumption that the device works in a reliably at all times. However, even the most well-known wearable devices do not publicly make known their accuracy values and other important specifications. Food and Drug Administration (FDA) in USA is responsible to make sure that the wearable devices are safe to use for human beings. Not all wearable devices are approved by the FDA. Many of us have been using the Apple Watch heart rate measurement. The Series 1 model of Apple watch, with its heart rate measurement feature, was released in 2016. This product was introduced to be used not for medical purposes, but for well being purposes, like monitoring heartbeat after workout. The device therefore didn’t need FDA approval. The first product for consumers that is FDA-approved for heart rate measurement is the Apple Watch Series 4 released in late 2018. Alphabet announced that FDA had cleared the Verily Study Watch as a medical device to record, transmit, store, and display electrocardiogram data soon after. The increase in FDA approval requests on wearable devices shows the viability and long
term health of the market for wearable products. The increase in the number of companies will then speed up the use of medical devices among regular consumers. [4].

**Power consumption:** Power consumption of wearable devices increase with advancement in technology. Older wearables with elementary functions (stopwatch, alarm clock, and calendar) had a long battery life. Current models with color and mostly touch displays, fitness trackers, heart beat monitoring, GPS tracking, and Bluetooth use much more battery power to operate, and thus require more frequent charging. Though the power consumption of these devices have reduced leading to an increased battery life, they still take up a majority of the area within a wearable system. With new blocks (cellular radios, new biosensors, and additional sensor analysis) continually being added to wearables, power consumption is still a critical issue for each of these additional features.

**Data transfer:** The signals acquired by sensors on a wearable device need to be transferred to be analyzed and possibly monitored by healthcare personnel. In a fully closed loop system, the communication may have to be two-way. The primary method of data collection for wearable devices is in real-time. Multiple methods such as wireless network technology ANT, Near Field Communication, Low Energy Bluetooth, WiFi, and cellular data transfer are being used in different devices. Among the aforementioned devices, WiFi and cellular data transfer have higher power consumption. One other encouraging methods is to transfer data by blinking light. This wireless mode of transmission is not visible to human eyes because of the high rate of blinking. Another approach, called seed and distribute, removes the need for each device to be connected to the internet and introduces devices relying on information from each other. This concept is being supported by long-promised multi-tiered networks, fifth-generation (5G) mobile communication systems. 5G communication is now available in many parts of the world and predicted to take over by the end of 2020. In this scheme, one device acts as a seed and distributes the common data of the devices.

**Security:** Unfortunately, the nature of these complex and heterogeneous Internet of Things (IoT) environments make dealing with their security issues very challenging. Furthermore, in these sensor networks, most nodes are resource constrained, which makes the property of the systems being lightweight necessary for IoT security mechanisms. Hence,
lightweight security seems crucial for the coming generation of sensors. Existing wearable devices store a large amount of confidential data. With the user having no control over this stored data, these companies can sell, release, or change the term of services if they go out of business. Security is an essential means to privacy. Encryption is becoming easier to implement and is now expected to be implemented in devices. Based on a recent study of common wearable devices, “If you’re not encrypting the data, you’re definitely not secure, even if you’re encrypting the data you can still not be secure.” [5]

**Materials, size, and flexibility:** This challenge is quite significant in the field of wearable devices and particularly the implementation of chemical sensors onto wearable devices. Finding appropriate materials to implement-high performance sensors is still a great challenge. Though chemical sensors have been around for a decade, they are often difficult to implement in terms of the material and size. Tissue, particularly in humans, is soft and flexible with complex deformations. Therefore, sensing chemicals directly on the skin needs soft materials that are flexible and malleable in multiple directions. To have the sensor response be as low noise as possible, soft tissue like sensors are essential. In many applications, such as implantable devices, the limitations and conditions for these materials are even more strict. These devices are costly to replace, invasive, and may damage the patient’s tissues or organs if they malfunction, leading to complications in the disease. Choosing materials and devices that are safe to have in the human body is therefore, a topic of much research [6].

### 1.1 Research Goals

This thesis addresses some of the challenges pointed out in the previous section. A novel secure sensor with the on-chip conversion of the physiological data to the frequency and implement on-chip security with real-time chaos signal ciphering is designed and verified. The sensors, temperature, and impedance, have a different rate of frequency, and the data sent to the ciphering block is chosen using an analog multiplexer. The analog hardware security, integrated on a chip, uses Lorenz equations to perform the encryption algorithm on the sensor output. The message is then transmitted, and a receiver decrypts the data.
To the best of our knowledge, this is the first experimentally demonstrated CMOS sensor integrated with encryption/decryption system. The overall proposed design of this system is shown in Fig. 1.2.

The integration of the full system on a single chip is also simulated in this thesis, implemented in 180 nm commercial CMOS technology, and tested experimentally. Having the sensors integrated with a chaotic system that ciphers data stream, the signals can be protected and secure while the device is being used. This security system, along with the temperature and impedance sensor, is advantageous over using a microprocessor or software based security since the whole system can operate with a magnitude of order lower power consumption.

1.2 Dissertation Overview

The rest of this thesis is organized as follows. In chapter 2, a literature review, on the three main part of work, temperature sensor, impedance sensor, and chaotic ciphering is done. Chapter 3 details the design of impedance sensor and presents the simulation and experimental results for this sensor. The sensor is tested for two applications (thoracic...
impedance measurement and hand gesture recognition) using human subjects. Chapter 4 develops the design and implementation of the second sensor, the temperature sensor. Simulation and experimental result for this sensor is presented in this chapter. In chapter 5, The mathematical equations of the Lorentz-based real-time encryption transmitter and decryption receiver, return map attack and chaotic shift keying are explained. The proposed design of a novel encryption/decryption circuit is included in this chapter, and the integration of the sensor with the ciphering block is described. Encryption and decryption circuits are the transmitter and receiver blocks of the sensor, respectively. Design and experimental results of a final on-chip encryption system are included in this chapter. Finally, in chapter 6, the conclusion is discussed and future possible paths outlined.
Chapter 2

Literature Review

Portions of this chapter are included in
“CMOS based whole cell impedance sensing: Challenges and future outlook.”
“A sub-µW CMOS temperature to frequency sensor for implantable devices,”

Based on new trending technologies in IoT and wearable devices, designing low power sensors are of great importance. Among the most important IoT and physiological sensors, impedance and temperature sensors can be named. Digital implementations of sensors can offer a higher accuracy and noise immunity than analog devices, which can encourage simpler, more compact systems. A low power quasi-digital sensors is developed, which combine the simplicity of analog devices with ease of use in digital devices and convert information into time, frequency, or duty-cycle, that are fitting for portable applications. Applications like wearable/implantable devices, industrial internet, smart grid, connected vehicles, and connected health are becoming increasingly popular, making IoT devices one of the hottest topics of recent years. Sensors are the most crucial building blocks of these systems. One of the main shortcomings of all of these integrated circuits is the lack of security that can be
implemented by data encryption/ciphering. In this chapter, along with a literature review on impedance and temperature sensors, a comprehensive look through the history of ciphering, and it’s future is done. Ciphering, as a tool for data communication, can be used on an integrated chip.

2.1 Impedance Sensor

Bulky benchtop instrumentation is the primary method of impedance sensing systems, a benchtop LCR meter is an example of this instrument [7]. As an example of application, benchtop lock-in amplifier was used in a real-time impedance measurement experiment to show that cells respond to prostaglandin immediately by showing a change in impedance but had a 2-hour delay in response to leukoregulin [8].

Impedance sensors are based on the application of Ohm’s law. In these sensors, either voltage is measured by applying current, or current is measured by applying voltage. In electrical impedance measurement, the sample between two electrodes are measured. This scheme of measurement is advantageous since it’s label free, non invasive and does not ruin the sample with the measurement process. Impedance measurement has application in measurement of different biological substances such as DNA, cells, and bacteria [9, 10, 11]. In pharmaceutical research, impedance measurement is an effective screening tool for new drug candidates. With biochemical and environmental agents, impedance sensing can quantify toxic substances [12, 13].

Detecting heart failure and pneumonia is another application of impedance measurement. Heart failure causes insufficient blood flow to organs with normal pressure. Acute decompensated heart failure (ADHF), results from deteriorating heart function and is a frequent cause of recurrent hospital admissions. Identification of those at risk for re-hospitalization is of prime importance. Many methods monitor symptoms that appear late. This increases the chance that the subject is sent to the ICU, which can be costly. Self-care for chronic heart failure, as a mean to reduce hospital visit, can be done by measuring intrathoracic impedance as a sign of fluid accumulations in the thorax [14, 15, 16].
Flexible, wearable trans-thoracic electrical impedance measurement systems to prevent heart failure are studied [17, 18, 19, 20, 21]. These electrodes can be implemented in patches and textiles. In [18], a 15cm×15cm patch sensor is proposed that monitors thoracic impedance and ECG with low-power and high resolution in a wearable low-cost cardiac healthcare system. Textile electrode implementation has a dry interface between the skin and the electrode resulting in an increased impedance in series with the current injecting electrodes [19]. Using stretchy textile material for improved contact has also been used [20], however, these materials may be less comfortable for elderly patients. The design proposed in [21] has electrodes to measure thoracic impedance implemented in a T-shirt. For better contact, ‘wet’ textile electrodes could improve charge transfer between the electrode and skin and facilitate better textile-based impedance measurement [22].

In the world of commercial thoracic impedance measurement, to the author’s knowledge, there have been no commercial FDA approved impedance sensors to detect thoracic impedance. A company called Corventis Inc. in 2009 developed a commercial impedance measurement system called, AVIVO Mobile Patient Management System [23]. This non-invasive system that was worn on the chest like a patch was used to detect of arrhythmia. The data transmission in this system was sent to a secure website using wireless devices and the medical professional was able to analyse this data regardless of the patient location. However, this company was later obtained by Medtronic, which changed this sensor from cardiac assessment to an implantable device (Reveal LINQ insertable cardiac monitor).

One other very interesting applications of impedance sensing the circuit is tested on, is recognition of hand gesture. This system can be used to control smartphones in the next generation of phone interfaces using impedance sensing bracelets or for translating sign language to text in real time. This application has been focused on by a few research publications in recent years. The first-hand gesture recognition sensors were designed with imaging systems, cameras would be set up, and pictures were taken of a single gesture and sent out for classification [24]. However, an imaging system requires a line of sight, heavy computational load, and expensive equipment. Thus, there is a need for cheaper, portable devices. In [25, 26] discrete hand gestures were recovered using an arm’s interior impedance geometry. This application, called Tomo (impedance measurement for tomography), is one
of the few systems that use a wearable system to recognize hand gestures. Among portable hand gesture recognition designs, there are other sensors modules which are utilized [27, 28, 29]. In [27], Jung et al. use air pressure sensors, which are large in size, allowing only a few sensors around the wrist. In [28], a polymeric strain gauge sensor is used to identify movements employed for rehabilitation, and [29] uses flexible capacitive pressure. These two sensors lack accuracy and recognize only a few patterns. In a more recent design, an FPGA implemented neural network along with commercial ICs were used for a high-performance hand gesture recognition [30]. To reduce computational load, power consumption, device area, and increase accuracy, an integrated impedance sensor is used. This sensor facilitates having more than 32 arrays around the wrist.

In this design, for both applications, a two-phase resistance and capacitance measurement circuit with a quasi-digital output is presented. Digital implementations afford a certain amount of accuracy and noise immunity, while analog implementations can encourage simple, compact systems. Compared to other temperature to frequency converters, this design consumes less power since it does not use any external clock and is implemented by a few blocks (Current comparator, Voltage Comparator, and XOR gate).

### 2.1.1 Impedance Sensing Circuits

The summary of impedance sensing is illustrated in Fig. 2.1 [31]. Having the the sample excited using a small signal is the initial step in all impedance measurement techniques [32]. One method converts the impedance of the sample to frequency or digital signal [12, 33]. In a commonly used method, the stimulating frequency is swept and impedance is measured in these frequencies [34, 35, 36]. These topologies measure the impedance by applying a current and voltage measurement, and vise versa. In this design, impedance is converted to frequency, eliminating switches and multiple current sources for a compact design.

The measurement principle of the first method is to get a frequency proportional to impedance. For this purpose, a current is periodically sourced and sanked through the impedance. In phase one, the current charges the impedance and impedance voltage level reaches an amount set by the high reference voltage. The reference voltage is responsible for switching the circuit from the charging to the discharge mode. In the next phase, the voltage
decreases because of the current discharging the capacitor until the voltage gain reaches a minimum set by the low reference voltage, and these two phases happen repeatedly. Fig. 2.2 shows the basic structure of an impedance to the frequency conversion system [12]. When Vout is high, $\phi_1$ is active, and $\phi_2$ is low. Therefore, the current, $I_0$, is injected through the electrode. This circuit has some extra switches such as $\phi_2$ that are placed between the supply voltage and ground to prevent a short circuit when the MOSFETs are active.

The time intervals that take the capacitor to charge and discharge determine the output frequency. The potential on the electrode increases as a switch, $\phi_2$ closes, and the current, $I_0$, is sourced to it. The capacitor potential is continuously being compared to $V_{refH}$ as it increases. This comparison will continue and will result in opening of $\phi_2$, once the potential reaches the high voltage reference, and $I_0$ is sunked from the electrode, decreasing the potential of the capacitor, until $V_{refL}$ is reached. To calculate the period of a single charge-discharge cycle:

$$T = 2\frac{C_e}{I_0}(\Delta V - 2R_eI_0) = 2C_e\left(\frac{\Delta V}{I_0} - 2R_e\right)$$  \hspace{1cm} (2.1)
where $R_e$ is the resistance and $C_e$ the capacitance of the cell. The change of the current through $R_e$ from $+I_0$ to $-I_0$ will cause a voltage drop related to $\Delta V = V_{refH} - V_{refL}$ and $2R_eI_0$ (Fig. 2.2).

The same method is used in [33, 37, 38]. [33] also digitizes the data using a D-flip flop for sampling the signal through the comparator. In [37], the frequency is generated by comparing the target resistance and capacitance to a known resistance and capacitance. The pulse through the cell was compared to a reference signal, which was generated by an SR-latch. The duty of this phase difference is then changed to a frequency using a multi-stage ring oscillator that can be stored as a voltage in a capacitor. In [38], the pulse through the cell was compared to a reference signal, which was generated by an SR-latch. The duty of this phase difference is then changed to a frequency using a multi-stage ring oscillator that can be stored as a voltage in a capacitor.

In the second method, the real and imaginary part of the signal is extracted by multiplying the signal with two signals that have a 90° phase shift. These approaches can be categorized based on whether they are voltage [39] or current based [32, 40, 41]. To increase the accuracy of the system, a zero detection block [42] or passive mixers [10] can be used. Moreover, on-chip implementation of pythagorator and arctangent modules can eliminate the need for
Figure 2.3: Lock-in approach in impedance sensing, voltage-mode lock-in amplifier sweeps the frequencies of the sinusoidal signal applied to the electrodes and measures the imaginary and real part of the output signal [39].

external digital signal processing [43]. The basis of this method is shown in Fig. 2.3. This method sweeps the frequencies of the sinusoidal signal applied to the electrodes and measures the imaginary and real portion of the output signal. The measured signal from the electrodes is multiplied by the $90^\circ$ and in-phase sinusoidal signal. The DC component proportional to the real and imaginary signals is obtained from the low pass filters [39]. The sinusoidal excitation is,

$$I_x = A \sin(\omega t + \theta) = a \sin(\omega t) + b \cos(\omega t)$$

(2.2)

Where the measured current at the xth electrode is shown by $I_x$, $A$ is the amplitude, and $\theta$ is the phase of the signal. In this equation, the real part of the signal is shown by $a = A \cos(\theta)$, and $b = A \sin(\theta)$ shows the imaginary part of the signal. By knowing a and b equations, the sensor’s impedance information is completely described. Therefore the phase and amplitude information of $I_x$ is extracted easily. Many CMOS implementations of impedance sensors utilize this method, where the real and imaginary impedance components are the output of the circuit, going to ADCs for full digitization [34, 35]. Since the impedance of a cell, a tissue or any physiological sample consists of real and imaginary portions, a stimulation pulse simulation can quantify this complex impedance.

Various impedance measurement devices use a digital signal processing block to evaluate the complex components of impedance derived, using lock-in amplifier approach. Many of these structures are based on voltage mode. However, there is a fundamental disadvantage
in using lock-in amplifiers in voltage mode, implementing an accurate pythagorator and arctangent in analog mode is very complicated. To solve this issue, current mode lock-in amplifiers are considered an effective substitute. By using this technique, the power consumption is very low, and the area is too small compared to the voltage mode because this technique does not need any external digital signal processing module [43].

One of the disadvantages of these systems is that by any minimal movement of the system phase from 90°, accuracy of the system suffers greatly. It is somewhat challenging to produce a sinusoidal signal, which is broadband and adjustable [44]. In [44], a battery-less miniaturized implantable device was proposed using a low-power bio-impedance system-on-chip sensor to measure impedance of the living tissues, which are variable from 2 kHz to 2 MHz. To solve the problem of having an accurate 90° phase difference, a passive mixer controlled by I/Q digital clock signals was used. Combining the lock-in approach with mixed signal approaches has also been proposed more recently [45]. In this method an ADC changes the impedance signal and turn it into digital data, where the real and imaginary part of the signal is extracted.

In a swept frequency lock-in approach, the signal must be passed through a low pass filter. Using low pass filters increases the measurement time at low frequencies. To have an improved system measurement time, a multi-frequency signal can stimulate the electrodes. To generate a multi-frequency sinusoidal signal, with frequencies that are spaced periodically, a silicon cochlea is used. These stimuli are added together and then sent as the input into the structure [46]. The “analyzer” part of the cochlea then takes this output and divides it into the related frequency to establish a relationship between impedance and frequency. In fact, using a silicon cochlea here creates an excellent filter bank, used as an “analyzer” (Fig. 2.4).

Recently, there have been various advancements in different areas of fabrication technology, and more complex circuits are needed to be designed with lower power consumption. In particular, for cell or tissue impedance sensing, multi-arrays, multi-function systems have been proposed. An array of more than 50,000 micro-electrodes have been used in [47, 48] to measure cell impedance and record physiological characteristics of a cell. The system is fabricated on a single chip, and using this system, position, adhesion, shape, and
other targeted physiological characteristics of a cell can be measured and monitored. In other approaches, multi-modality arrays have been proposed that measure more than one parameter on the same chip [49, 50]. However, having systems with the ability to measure different parameters will increase the area as well as the power consumption of the system. Even in the case of using a single readout system for multiple sensors, encoders, decoders, multiplexers, and even memory units need to be considered, which adds to the system's complexity. This, in turn, makes the system slower, adding to the complexity of designing a system-on-chip multi-modal sensor.

### 2.2 Temperature Sensor

Human body signals can be measured using wearable sensors. Using a wearable sensor, quality of care, and daily life rises significantly. Because of progress in micro and nano-fabrication technologies, the integration of wireless and passive sensor systems into wearable systems is becoming more common. This integration leads to the reduction of device failure rates, since one of the first signs of device malfunction can be detected in real-time. Having multiple sensors on wearable devices also offers the potential to diagnose and treat health issues in real-time. These advanced sensor systems must be small in size, be low-power, and
enable wireless data transmission. An ideal sensor system should be simple and robust, and should have a minimal probability of malfunction and failure.

In the case of implantable devices, these characteristics even become more strict. When sensitive biological cells and tissues are overheated due to being close to an implantable device, tissue damage occurs. The designers of implantable systems thus have in mind to restrict heat generated around a tissues to less than 1 °C by setting a limit on power consumption and consequently, power loss. The amount of power that can safely be dissipated depends on the physical characteristics of the device. Mostly, shape and size can determine the safe power dissipation, small devices can safely disperse smaller powers.

Moreover, there are not much data available on blood stream heat transfer, unlike body heat transfer, which can be accurately simulated. It has been shown that a 100-electrode array implanted layer with circuit sizes \( \approx 6 \text{ mm} \times 6 \text{ mm} \times 2 \text{ mm} \) dissipates approximately 10 mW or 100 \( \mu \) per electrode [51]. 100 \( \mu \) of power consumption includes amplifiers, data converters (digital to analog or the other way around), biasing and controlling circuits, and references needed on a chip. In the design of a temperature sensor, especially one with application in medical and wearable devices, power consumption should be kept low to prevent adding to overheating. To satisfy this restriction, power consumption must be limited to sub-\( \mu \)W. Therefore temperature sensors are crucial blocks of any sensing systems.

Commercial wearable temperature sensors are common since they are used to monitor fever, especially in infants. TempTraq [52] is the first Bluetooth, wearable temperature monitoring systems. This single-use device is a soft, comfortable patch that continuously monitors body temperature for up to 48 hours. The patch sends the reading as well as alerts to compatible mobile devices. TempTraq is purposed to monitor the patient’s temperature without Disturbing them. Fever scout by VivaLNK [53] is a multi-use wearable thermometer patch that is worn under the arm, where it continuously monitors body temperature. The measured temperature can be sent up to 100 feet away to a smartphone through the accompanying app. This 41 mm by 61 mm path can create alarms if a temperature threshold is defined. This patch is purposed for post-operation fever, flu infections, child fever, and drug effects. Fever scout is water-resistant and has a battery life of up to 1 week per charge.
Though these sensors are promising, in order to have these sensors arrayed with other sensors or systems, and be used for a longer time without the need to change/charge, the power consumption should still be reduced, reaching sub-$\mu$W realm. In this design, a temperature sensor using weak inversion MOSFETs and a quasi-digital output is presented. Digital implementations afford a certain amount of accuracy and noise immunity, while analog implementations can encourage simple, compact systems. Compared to other temperature to frequency converters, this design consumes less power since it does not use any external clocks and biasing.

### 2.2.1 Temperature Sensing Circuits

Recently, various low power temperature sensors have been reported. First designs of integrated temperature sensor used bipolar junction transistors (BJTs) in their design. A BJT can be considered to be a current controlled voltage source. Using a stable/fixed biasing current, as the temperature rises, the voltage between the emitter to base decreases. A voltage insensitive to temperature is used. The temperature is measured and calibrated by comparing it to this voltage. This method is shown in Fig. 2.5.

However, their (typical) hundreds of $\mu$W power consumption reduces its practical implementation for miniaturized, wearable and portable sensors. BJT based sensors are generally self referenced since the difference between the collector currents of two BJTs is proportional to absolute temperature (PTAT). However, these sensors need a high accuracy
ADC for the temperature measurement to be more precise. In [54], a sigma Delta modulator is used as an ADC because of its high resolution in lower frequencies. Different topologies of sigma Delta modulators have been considered in temperature sensors. The use of many operational transconductance amplifiers (OTA) in sigma Delta modulators makes them bulky and power hungry. This design tries to relax the bias issue of sigma Delta modulators by using a self-biased OTA. However, even with this OTA, the power consumption is a few magnitude of order higher than the sub-μW target. Generally, an accurate ADC uses significant amounts of power and can require a large area on chip to compensate for the process variations typical in CMOS technology. The majority of sensors designed using this method showed better than 1°C accuracy and a few hundred μ watts of power [55, 56, 57]. A BJT based on-chip temperature sensor incorporating an ADC has been demonstrated in these designs.

Reference clocks, along with a temperature-dependent frequency circuit, have also been used as temperature sensors. Clock based temperature sensors generally have less resolutions and accuracy for the benefit of less power consumption [58, 59, 60, 61]. A block diagram of this method is shown in Fig. 2.6. Most of these designs use an external clock, not convenient to have with portable devices. Clock-less temperature sensors converting temperature to delay or pulse width with low power consumption have also been reported [62, 63, 64]. In [65], a temperature to current converter generates a current that depends on temperature (Fig. 2.7). This output current, ideally proportional to temperature, is then converted to frequency by an oscillator which is current controlled. Therefore the oscillations frequency is proportional to PTAT and that leads into the dependence on absolute temperature. Calibration systems can be incorporated, however, having a good calibration system increase the accuracy in cost of power consumption and area.

MOS devices working in weak inversion enable ultra-low power operation. The power consumption of these devices can go as low as few tens to few hundreds of nW. An example of this group is designed in [66]. In this paper, the goal of sub-μW power consumption is set, and the sensor consumes only 220 nW at room temperature under continuous operation. The work in [67] achieves the low power consumption of 600 nW by using dynamic threshold voltage MOS transistors (DTMOSTs) as the sensing device. However, having any MOSFET that uses special steps in the fabrication process, can make this process costly. The use of
modified voltage to current converter, current mirror structures, and a new sensor topology in [60] reduced the power consumption to ultra-low power of 71 nW. Serially connected sub-threshold MOS transistors, implemented as a sensing device, enabled a CMOS temperature sensor to have a power consumption of 119 nW [62]. In [68], the ratio of the currents of two Mosfet transistors biased at different \( V_{DS} \) values and operating in weak inversion is a linear approximation of an exponential. The \( V_{GS} \) of two transistors is kept the same but apply different \( V_{DS} \)'s. By having one \( V_{DS} \) much larger than \( V_T \) and one \( V_{DS} \) below \( V_T \), the current ratio provides a linear and sensitive relation to temperature. This structure is shown in Fig. 2.8.

In applications that have a limited temperature range and small variations that are important to us (dynamic memory, implantable devices), accurate measurements for every temperature is an overkill. In [69] this design, named folded temperature sensor (Fig. 2.9), temperature references are generated by resistor ladders. These references can be designed to define a few separate threshold limits for temperature sensing. In each of these threshold limits, the temperature sensor does an accurate measurement, by moving to a different range,
a new segment in temperature sensing is started. This segmented temperature sensing leads to a reduction in supply voltage. The sensitivity and limit of each of these sections can be changed, by alignment of these segments, reference circuits can be simplified.

Overall, there are significant advantages afforded by time or frequency-to-digital conversion [58, 62, 64, 70, 71]. Having a BJT-less temperature to frequency/digital structure used in this design can take advantage of having a low power design, by use of Sub-threshold MOSFET transistors and removing the need for external clocks and power consuming ADCs.

### 2.3 Chaotic Ciphering

Encryption has two basic types of asymmetric and symmetric key encryption. Symmetric key encryption is an older and more well-known method. An example of symmetric key encryption is to shift each letter alphabetically. Using the key of +2, ”Ava is a spy” will become ”CXC KU C URA” and transmitted. The receiver will shift the letter back by -2
and have the message decoded. This method has its own limitation, like the transmitter and receiver using the same key and the need to securely notifying the receiver of the key. Enigma, One-time Pad, Stream Cipher, and Block Cipher are among different methods of symmetric key encryption. The security of symmetric key encryption depends on selectively sharing of the private keys.

Another method of encryption, eliminating this weakness, is asymmetric key encryption. In this method, the key and algorithm for encryption and decryption are different from each other. In asymmetric encryption, the key for encryption is made public, but the key for decryption is only known by the receiver and not by the third party. This method depends on the existence of one-way function. An example of these one-way functions is $y = \log(x)$, securing a message $y$, is easy using this function, $x$ can simply be calculated as $10^y$, however given $y$, $x$ can be calculated if you have a calculator. If $y$ is a long key with a few hundred bits, even a handheld calculator is not enough to decipher the code [72].

Cryptography is a fundamental part of all online communication, wearable and implantable devices, and smart vehicles. Many commonly used cryptosystems are expected to fail once large quantum computers exist. Quantum computing started in the 1980s and utilize phenomena relating to quantum-mechanical such as superposition, principle of uncertainty, wave–particle duality, and entanglement to perform computation. The first quantum computing theory was given in 1980 based on a model of the Turing machine [73]. Later it was suggested that computers that perform quantum computation are known as quantum computers. In October 2019, Google in partnership with NASA, claimed that they have achieved quantum computing [74], though this claim raised some dispute [75, 76], it is still one of the most impressive milestones in quantum computing. Quantum computers can break the cryptography keys quickly by exhaustively trying long bits of all secret keys. Therefore, methods of security other than symmetric and asymmetric security are gaining more importance, while we are getting closer to quantum computing and breaking all means of ciphering. Chaos is a method of ciphering that existed from 1970s but being reborn in the recent years with IoT and wearable devices enforce security that can be implemented with low power electronics.
2.3.1 Chaotic Ciphering Circuits

Controlling chaos was first achieved by the simple “OGY” algorithm published in 1990 [77]. Chaos synchronization is when transient trajectories of the two identical chaotic systems approaches one, even when the initial condition is different. Chaos is a complex, unpredictable dynamic system which is characterized most commonly as extremely sensitive to the start up conditions. Under specific conditions a chaotic circuit can produce a correlated response, when driving a similar system. Chaos synchronization is the base of using chaos in communication.

As early as 1993 [78], synchronization of Lorenz-based chaotic circuits was presented with applications in communications. Instead of conventional frequency synthesizers, chaos generators can be used as communication carriers. Here the chaotic signal is modulated by the transmitted digital data, and the digital signal is transmitted with noise-like spectral properties of chaos.

Chaotic secure communication is advantageous in terms of having a strong real-time performance, but the implementation of these systems is still scarce, and chaotic secure communication is still not widely (if at all) commercially implemented. Most researchers are studying chaos theory in numerical simulation. However, communication schemes are challenged by the need to maintain synchronization when dealing with large signals. The lack of implemented circuits and experimental results prevents us from drawing the right conclusions regarding chaos implementation. Therefore, In this section, the literature review, goes through the chaotic systems that have a means of implementation from discrete parts or analog CMOS fabrication with a brief mention of digital implementation, regardless of the application. Generally, Chaotic encryption has been implemented using common software platforms with a few hardware implementations. Hardware platforms having a small on-chip area and minimum power, unlike software, can be an efficient solution. Moreover, a dedicated chip can have a much higher speed for data processing than a microprocessor running a software platform.

In 1995 [79, 80], implemented one of the first experimental verifications of chaotic encryption using a $g_m$-C modulator/demodulator analog CMOS IC is implemented. In
2002 [81] a monolithic chaotic oscillator is proposed capable of exhibiting double-scroll-like chaos. The system uses a canonical mathematical model, a model controlled using a single-parameter. This oscillator relies on the very simple idea of digital inverter developed by two-transistor, having a natural and robust nonlinearity.

In 2009 Trejo-Guerra et al. [82] verified the synchronization process of two Chua’s current conveyor based oscillators experimentally, by implementing a master-slave communication system. In 2010 [83], n-scroll attractor parameters is approximated by the nonlinear system parameters along with real physical active device parameters. In 2012 Trejo-Guerra et al. [84] presented integrated circuit generating 3- and 5-scroll attractors. Multi-scroll chaotic designs implemented discretely has the significant drawback of needing a number of external DC reference sources. Therefore, the design proposed by Trejo-Guerra highlights the integrated circuit (IC) realization of a multi-scroll oscillator with 3- and 5-scroll attractors without the disadvantage of having numerous external DC references. Trejo-Guerra et al. in 2013 [85] also address the problem of having multiple dc references in Multi-scroll-attractors. The voltage to current converter proposed in this design use inverters that eliminate offset by having capacitors on gate.

Other than Chuy’s based attractors, Loretz equations are an alternative method of signal ciphering for communication security. These voltage equivalents of the chaotic equations, CMOS fabrication of Lorentz chaotic oscillator, as the source of chaos goes back to 1999 [86]. The baseband chaotic encryption/decryption system was designed and fabricated using the CMOS technology as a more recent integrated implementation. Wu et al. [87] combines Lorenz and Stenflo equations to provide a four-dimensional system. This system has less number of elements and reduces power consumption.

After a review on chaotic circuits, here the focus is on the circuits used in communication of signals, since not all chaotic oscillators are suitable for communication. In recent years, many circuits implementation of chaos has been presented. Only a couple of these systems are fabricated, and in most cases, only simulation results or the implementation of the circuit with discrete parts are studied. Almost all of these methods show practical difficulties in terms of accuracy and mismatch of components. Since the component parameter values drift with age, power-supply spikes, and temperature, the designed chaotic circuits,
must have accurate components. Because of this sensitivity, only by having matching components between transmitter and the receiver, information recovery can be ensured. By implementing chaotic circuits through fabrication, the mismatch and noise are reduced, giving the opportunity to have secure communication in higher frequencies.

Chaotic generators implemented in digital hardware is an alternative means of chaotic synchronization. These systems, though they mitigate issues with mismatch of the parameters between the two transceivers, they still struggle with channel noise. Digital implementation like FPGA chips architecture can be used to implement others chaotic systems including Chua, Lü, Rössler, and Chen. However, having a digital system to use with wearable and IoT devices is not feasible. In IoT devices with an increase in the number of nodes, having a micro-controller for each node to cipher signal can be costly. For wearable and implantable devices, digital systems are far too power-consuming to be used.

Information security is a serious challenge, particularly for medical devices. In the case of implantable devices, any attack can be fatal. Adding security to these devices is also critical since they are usually battery powered and with limitation on area, power supply and area. All of these issues make the usual security procedures difficult or impossible to realize. Few security methods have been used in medical device’s communication. One method is authentication, where the destination device requesting a communication can be identified using temporary or permanent shared keys or ancillary sensors like biometric signal collectors. Another method is anomaly detection, where the data received and sent by the device is observed and analyzed. Another secure communication can use cryptography or ciphering that relies on a shared key that is not understandable by a third party. Among different methods, with the advancement of Moore’s law and possibility of implementing more complex circuits in a limited space, use of a chaotic system in ciphering is drawing more and more attention.

There have only been a few security implementations that can be used with bio-medical devices. In [88, 89] a Henon Map was used to generate the Pseudo-Random keys, shared by the transmitter and receiver. In this proposed method, the output key is not exchanged wirelessly but set/preset as an initial condition between the devices, which is the benefit of the proposed Pseudo-Random generators. The generator generates the encryption key
using two inputs. These are the data (exchanged wirelessly) and the key (not wirelessly exchanged). Without knowledge about one of the inputs, recreations of a similar sequence is impossible. This implementation, through chaos-based, still fits in the group of public keys with the length of 128 bit that is breakable by a high-speed computer.

To have a better understanding of the systems implemented so far for chaotic communication, systems that have mentioned use-ability in communication and have means of hardware implementation are studied. In 1995, [79, 80] presents the first experimental verification of chaotic encryption gm-C modulator/demodulator analog CMOS IC that implements a 3rd-order nonlinear differential equation. This implementation is based on Chuy’s equation. These on-chip efforts on Chuy’s implementation of chaos however, involved nonlinear resistor that requires a considerable design effort. The area consumed by these resistors were big and large supplies were needed.

One of the first analog implementation of chaos as a cryptosystem working at baseband frequencies is designed in [90]. This design works at lower frequencies rather than close to reality wireless range frequency. The Lorenz based cryptosystem was implemented using a 1.2µm technology. The next design in 2005 [91] used a discrete-time chaos generator implemented with two nonlinear circuit cells. The design is implemented in 1.2µm technology and is the smallest due to a few number of transistors used. However, this scheme can’t be used in transfer of analog signals, though applicable in transfer of bits using chaos. No other design of this family will be considered since it can’t be utilized in transfer of sensory signals. In [92], a digital hardware implementation of chaotic generators is demonstrated in Fig. 2.10 in the FPGA world, where no mismatch exist between transmitter and the receiver. Another advantage compared to discrete devices is that the noise only depends on channel noise sensibility. A similar implementation with FPGA but a different function is implemented by [93]. Here, as seen in Fig. 2.11, the units of the oscillator determine the algorithm’s coefficients. The y unit multiplies k0, k1, k2, k3, k4, and k5 values with contents in the algorithm and obtains the output of the oscillator [93]. These are then sent to filter to eliminate errors in the output. These methods are still very power consuming and not a viable solution for portable devices.
Chen et al. [94] uses Lorenz equations to implement a discrete circuit that can synchronize slower signals used a master transmitter and a slave receiver. Though showing good results in circuit simulation, a discrete systems with a few ten components is not a good solution for warble devices. The schematic of this system is similar to what have been proposed in [87], using integrators and multipliers to implement chaos. The schematic shown in Fig. 2.12 is an implementation a four-dimensional modified Lorenz-Stenflo system. This paper shows nonlinear dynamic characteristics of system by Lyapunov exponent extraction and develops the system with a fewer elements. The design is implemented on a chip using 0.35 \( \mu m \)
Figure 2.12: Chaotic oscillator architecture proposed in [87].

process for the encrypted communication application. The results does not show fabricated chip results but stays at simulation level.

In [95], to improve Lorenz chaotic system, Xiong et al. uses active control method. Utilizing this method, the synchronization error system can be stabilized from the origin. Here, synchronization of state between a transmitter and a receiver is implemented for secure communication. This communication based on chaotic modulation is generated by a synchronization link between the transmission/receiver channels. In the proposed scheme, an improved Lorenz system is used as a chaos generator. In this design, secure communication by chaotic modulation is implemented by using analog multipliers, operational amplifiers, resistors, and capacitors, a close design to what demonstrated in Fig. 2.12. This design is implemented using discrete parts, not low power, and small enough for wearable devices (Fig. 2.13). In [96], a low-voltage CMOS implementation of the double-scroll chaotic system
Figure 2.13: Circuit board photo of oscillator unit to see the size and number of components for a discrete chaotic ciphering transmitter [94].

using OTAs is introduced. This method removes the need for resistors and other passive components that are tuneable electronically by external currents even after integration on-chip. The schematic of the system, Fig. 2.14, shows the OTA based design and development of nonlinearity with transconductance. Though the system is implemented in 0.35µ CMOS technology, this system is not fabricated, and all the experimental results are extracted from Matlab Simulink and HSPICE. The newest development is [97], which uses the same circuit implementation as shown in Fig. 2.14 but with one less state. This chaotic oscillator uses MOSFET technology. This makes it more resilient with regards to process, voltage, and temperature or PVT variations. In this paper ([97]), two designs of Lü’s chaotic oscillator were demonstrated, and layout and post-layout simulation presented, however, the system is not fabricated. All of these designs are compared in a table in section 5, and a Figure of Merit (FOM) is extracted to be able to have a better comparison between these chaotic circuits that have application in communication.

Though there have been various efforts in the implementation of chaotic communication systems, both in digital and analog electronics, there is still no system implementation that is suitable to have as a part of portable devices. The designed system is lagging in term of being low power, low area, and reliable. With quantum computing in the horizon and the
failing of known symmetric, asymmetric ciphering available for wireless devices, having an analog implementation of ciphering integrated on-chip is a topic that will draw more and more attention in the coming years.

### 2.4 Conclusion

Considering the literature, a low power, low area impedance sensor that can be arrayed and does not need ADC blocks can be incorporated in many applications. In temperature sensors, power consumption and accuracy are of great importance. With the advancement of technology, sub-µw temperature sensors are being developed that push the accuracy toward a tenth of °C. Temperature sensors are a good add-on to any system to monitor the functioning of electronic parts. In wearable devices, especially implantable devices, the rise of the device’s temperature should be closely monitored to prevent harm to sensitive body parts. Besides area and power consumption, security is a crucial, mostly ignored aspect of sensors when it comes to data transfer. Chaotic ciphering, implemented on-chip, seems a viable solution for the incorporation of security on sensor devices.
Chapter 3

Impedance Sensor

Portions of this chapter are included in

3.1 Design

Fig. 3.1 shows the impedance to frequency conversion circuit. The input is an alternating AC voltage that stimulates the cell. The cell is considered to be a complex impedance with resistance and capacitance. This system eliminates the need for the switches or multiple (sink and source) current references that are common in impedance to frequency designs. The operating modes are divided into resistance and capacitance measurement mode. In resistance mode, the alternating voltage will be changed to an alternating current signal, with amplitude proportional to the resistance. The current is,

\[ i = \frac{v_a \sin(\omega t)}{R} \]  (3.1)
where $v_a$ is the amplitude of the excitation signal, $R$ is the cell resistance, $\omega$ is the frequency, and $i$ is the current through the cell. When the output of the comparator is high, the difference between the reference current ($I_0$) and the measured current is positive, thus, 

$$I_0 - \frac{v_a \sin(\omega t)}{R} > 0.$$ 

The pulse width of the high signal is then,

$$T_R = \frac{\sin^{-1} \frac{I_0 R}{v_a}}{\omega}$$

where $T_R$ is the pulse width.

The reference is chosen based on the targeted range. For this application the equivalent current of 0.5 V going through 10kΩ was chosen as the reference. With these values, a 10KΩ will give the duty cycle of 0 %.

The capacitance measurement mode is based on phase delay detection. The signal, delayed by the capacitance of cell, is connected to one comparator, and the AC signal goes to the other comparator. Since the delay is better detected in lower voltages, the voltage reference is a small voltage just to keep the transistor on. The difference of the original and
delayed signal phase \((\phi)\) and the pulse width of capacitance output is,

\[
T_c = \phi = \tan^{-1}\left(\frac{j\Delta C \omega}{R}\right)
\]

(3.3)

where \(T_c\) is the pulse width and \(\Delta C\) is the change in capacitance.

The SR-latch acts as a high frequency modulator. An input square signal with a higher frequency is connected to the reset pin of the SR-Latch. A higher bandwidth will result in a higher frequency at the output of the latch. The Fourier series (for \(n \in \text{odd}\)) of resistance signal can be written as,

\[
x_R(t) = \sum_{-\infty}^{\infty} \frac{1}{j \pi n} e^{j 2 \pi n t / T_R}
\]

(3.4)

and the Fourier series of the reference signal (for \(n \in \text{odd}\), assuming a pulse width \(T_{\text{ref}}\), is,

\[
x_{\text{reference}}(t) = \sum_{-\infty}^{\infty} \frac{1}{j \pi n} e^{j 2 \pi n t / T_{\text{ref}}}
\]

(3.5)

Therefore the ratio of the frequency of the reference to the measured resistance (for \(n \in \text{odd}\)) is,

\[
n_{\text{pulse}} = \frac{\sum_{-\infty}^{\infty} e^{j 2 \pi n t / T_R}}{\sum_{-\infty}^{\infty} e^{j 2 \pi n t / T_{\text{ref}}}}
\]

(3.6)

where \(n_{\text{pulse}}\) is the number of pulses in a given time period.

The proposed current comparator is based on [98, 99]. A current-mode comparator determines if a received input signal (in the form of a current) exceeds a reference or predefined threshold current, and produces a voltage based on this comparison. Generally, current comparators are used in high-speed applications such as nonlinear current-mode signal processing and A/D converters. High resolution is another feature of current comparators that can be useful in current-mode image compression chips. The design reported in [98] proposed by H.Traff in 1992 is a low input impedance current comparator that led to broader use of them. This design is low power and well suited for high-speed applications.

If the sum of \(I_{\text{in}}\) and the reference current applied to the comparator is positive, \(V_1\) goes high and is amplified by \(M_2\) and \(M_4\) (here the assumption is that \(M_1\) has initially turned
### Table 3.1: Transistor sizing for different blocks.

<table>
<thead>
<tr>
<th>Block</th>
<th>Transistor</th>
<th>W/L (µm/µm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Comparator</td>
<td>M1, M4, M6-7</td>
<td>0.88/0.36</td>
</tr>
<tr>
<td></td>
<td>M2, M3, M8</td>
<td>0.48/0.36</td>
</tr>
<tr>
<td></td>
<td>M5</td>
<td>4.0/0.36</td>
</tr>
<tr>
<td>SR Latch</td>
<td>M1-M4</td>
<td>0.28/7.0</td>
</tr>
<tr>
<td></td>
<td>M5-M8</td>
<td>0.8/7.0</td>
</tr>
<tr>
<td>XOR Gate</td>
<td>M1-M3-M5</td>
<td>4.0/1.0</td>
</tr>
<tr>
<td></td>
<td>M2-M4-M6</td>
<td>2.0/1.0</td>
</tr>
<tr>
<td>Voltage Comparator</td>
<td>M1-2, M5-6, M10-13, M16-17, M20</td>
<td>1.0/0.5</td>
</tr>
<tr>
<td></td>
<td>M3-4, M7, M14-15, M19</td>
<td>2.5/0.5</td>
</tr>
<tr>
<td></td>
<td>M8-9, M18</td>
<td>1.5/0.5</td>
</tr>
</tbody>
</table>

M$_5$ – M$_8$ are just two inverters used to give a rail to rail output voltage signal. Based on the current direction to the comparator, the gate of M$_5$, M$_7$ would have either a low or high impedance path to ground translated by the two inverters to a low or high voltage, respectively. When the input of the inverters is a high impedance node, and with the gate of the inverters drawing almost zero current, the voltage is close to the voltage connected to the input current (VDD), which causes a high voltage at the output of the second inverter. Using the two inverters facilitates the connection of this voltage signal to the next stage while mitigating loading effects.

The voltage comparator is standard, with a preamplifier, decision, and gain stage (Fig. 3.1). Positive feedback from the cross coupling of M$_{10}$ – M$_{13}$ increases the gain of the decision element. A CMOS NAND gate based on SR-Latch is used as the output stage. In this design, transistors are sized to work in an ultra-low power regime of 3 nW. The latch has a full-rail fast swing, compatible with the switching rate of 10 MHz. A transmission gate XOR is used. All transistor sized is shown in Table. 3.1. The transistors are primarily sized for low power consumption.
3.2 Simulation and Experimental Results

The designed impedance measurement system was tested both through simulation and experimentally to confirm the functionality of the circuit. In all experiments HEWLETT PACKARD, 33120A waveform generator is used to generate the stimulating sinusoidal voltage. Agilent E3831A is used to supply the DC voltages, and all signals are recorded using Agilent technologies-X3104 A Storage Oscilloscope.

3.2.1 Resistance Sensor

As noted in section II, the first block of the resistance measurement system is a current comparator. The simulation results for the characterization of the current comparator is shown in Fig. 3.2. For doing the DC characteristics in the current comparator, in Fig. 3.2(a), one input is connected to 6 $\mu$A and a sweeping 4 to 8 $\mu$A on the other, showing an output change of GND to VDD on 6 $\mu$A. In Fig. 3.2(b) the positive input is swept from 4 to 8 $\mu$A, while the negative input is stepped from 4 to 8 $\mu$A in 1 $\mu$A increments. As is shown in Fig. 3.2(a), the offset is about 0.2 $\mu$A. The derivative of this plot shows the gain of this comparator (Fig. 3.2(c)). As it is shown, AV is about 4 M.

The designed current comparator was simulated to confirm the functionality of the circuit. Constant current and a sinusoidal reference were used as inputs. As depicted in Fig. 3.3, the output pulse is low when input current is lower than reference and is high when input current is higher than the reference. The plot is shown for 1 $\mu$A and 8 $\mu$A.

To test the circuit experimentally, a sinusoidal voltage source with a 0.5 V amplitude and frequency of 1 kHz was used as one input, and the other input was a changing DC voltage, both going through 5 K resistors. The transient response of the circuit is shown in Fig. 3.4. In Fig. 3.5, the output is tested for different values of resistance, which confirm the linearity of the impedance measurement circuit in a large range. Published values for the resistances range from $10^2$ $\Omega/cm^2$ to $10^5$ $\Omega/cm^2$, with most around 1 k$\Omega/cm^2$, and as seen in Fig. 3.5, the circuit is functional in this range. The capacitance is usually given as around 0.1 $\mu F/cm^2$, with published data between 0.1 $\mu F/cm^2$ and 1 $\mu F/cm^2$. As a separate test, the capacitance of the cell was changed too low (1 pF) and too high to see if the system can
(a) Single input current comparator sweep

(b) Multiple input current comparator sweep

(c) Gain of the current comparator.

Figure 3.2: Current comparator characterization using DC sweep. (a) Current comparator having 6 $\mu$A on one input and a sweeping 4 to 8 $\mu$A on the other, showing and output change of GND to VDD on 6 $\mu$A. (b) Positive input is swept from 4 to 8 $\mu$A, while the negative input is stepped from 4 to 8 $\mu$A in 1 $\mu$A increments. (c) Gain of the current comparator.
detect a bad connection to skin; in this case, the resistance measurement changed to a flat line.

As explained in previous section, to change bandwidth to the frequency a reference with a higher frequency and an SR-latch was chosen to modulate the pulse-width to frequency. The next block tested experimentally is the SR-latch. The output of the SR-latch is shown in Fig. 3.6. As depicted when the set signal is high, the output is high, and when the reset is high, the latch is reset. This block is tested with a VDD as low as 0.5 V to show the functionality of latch even with small changes. In this design, the time reference was 10 MHz, which leads to having a different number of pulses based on the bandwidth. The accuracy of the system can be raised if a higher frequency is used as the SR-latch reference.

To see the linearity of this system, output frequency was measured for 10 Ω to 10 kΩ input impedance at every 1 kΩ. The experimental results are shown in Fig. 3.7.
3.2.2 Capacitance Sensor

To test the capacitance measurement system, the reference AC stimulating signal is passed through a reference resistance and an impedance that is consisted of resistance and capacitance. Since the signal going through a capacitive element changes the phase, voltage comparators can be used to detect a constant voltage crossing.
Figure 3.6: SR-latch output showing high output when set signal is high, and low output when reset is high.

Figure 3.7: System output frequency for different impedance.

For DC characterization of voltage comparator (Fig. 3.8(a)), the positive input is swept from 0 to 1 V while the negative input is stepped from 0 to 1 V in 100 mV increments. The derivative of this plot shows the AV of this comparator (Fig. 3.8(b)). As it is shown, AV is about 10000. This change in phase is changed to duty cycle using an XOR gate. To see the linearity of the system, output frequency was measured for 10 nF to 200 nF input capacitance at every 10 nF. The simulation results are shown in Fig. 3.9.

To test the capacitance measurement system, the reference AC stimulating signal is passed through a reference resistance and an impedance that is consisted of resistance and capacitance. Fig. 3.10 shows the transient response for 100 nF that has a duty cycle of 90
Figure 3.8: Voltage comparator characterization using DC sweep. (a) Positive input is swept from 0 to 1 V while the negative input is stepped from 0-1 V in 100 mV increments. (b) Gain of the current comparator.
The duty cycle was also recorded for 50 nF and 33 nF, which showed the duty cycle of 45 µs and 30 µs, respectively. The system layout was done in 180 nm-CMOS technology. This technology has a MiM Capacitance of 2.0 fF/µm², between $M_5$ and $M_6$, and has a die thickness of 12 mils. This CMOS process offers up to 6 metal layers. It can be seen from Fig. 3.11 that the total area of the system does not exceed 300 µm². Fig. 3.12(a)) and Fig. 3.12(b)) show the result of measuring a complex impedance. In Fig. 3.12(a)) resistance measurement is done while having 3 different capacitance, and in Fig. 3.12(b)) capacitance is measured while having 3 different resistance. This shows an ignore-able counter measurement while having complex measurement.

The noise measurement was done using SR785, showing an average noise density of 12 µV/Hz in the 10 Hz to 100 kHz frequency range. The sensitivity of this sensor depends on the reference input of the SR-latch stage, making the resolution of the system tune-able. In this system to be compliant with transmitter frequency rate (433 MHz), the signal reference was chosen 10 MHz, switching up to 1000 times in the 1ms bandwidth of the signal. Each output pulse of the output stage of SR-latch is therefore associated to a change in 0.5 Ω of impedance change. The comparison of the designed circuit to recently published papers is shown in Table. 3.2. The data illustrated is per channel data. The table shows that with a power consumption in the same range of the sensors with lowest consumption, this sensor has a improved error and consumes less area.
3.2.3 Human Experiments

The designed circuit is then tested for two applications of thoracic impedance measurement and real-time translation of sign language. In this system, in order to make a simple and easy
(a) Resistance measurement with 3 different capacitance values.
(b) Capacitance measurement with 3 different resistance values.

**Figure 3.12:** RC simultaneous measurement showing (a) a change in resistance measurement with 3 capacitance values, 10 nF, 47 nF, and 100 nF and (b) a change in capacitance measurement with 3 resistance values, 1 kΩ, 5 kΩ, and 10 kΩ.

**Table 3.2:** Comparison table with state of art impedance measurement.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Range (Ω)</th>
<th>Tech (µm)</th>
<th>Area (mm²)</th>
<th>Power (µW)</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[10]</td>
<td>20-2.5 k</td>
<td>0.13</td>
<td>0.025</td>
<td>82</td>
<td>1%</td>
</tr>
<tr>
<td>[12]</td>
<td>1-10 k</td>
<td>0.35</td>
<td>2</td>
<td>200</td>
<td>~10% Reliability</td>
</tr>
<tr>
<td>[34]</td>
<td>500-4 k</td>
<td>0.5</td>
<td>0.06</td>
<td>6</td>
<td>RMS err 0.027</td>
</tr>
<tr>
<td>[35]</td>
<td>-</td>
<td>0.18</td>
<td>2.7</td>
<td>8</td>
<td>0.41 % R mode 0.73% C Mode</td>
</tr>
<tr>
<td>[44]</td>
<td>1-10 k</td>
<td>0.35</td>
<td>0.007</td>
<td>150</td>
<td>0.28% Mag 0.12% Phase</td>
</tr>
<tr>
<td>[45]</td>
<td>1-1 k</td>
<td>0.35</td>
<td>19.38</td>
<td>100000</td>
<td>0.8%</td>
</tr>
<tr>
<td>[46]</td>
<td>~ 1-1 k</td>
<td>0.5</td>
<td>4</td>
<td>30</td>
<td>2%</td>
</tr>
<tr>
<td>This work</td>
<td>1-10 k</td>
<td>0.13</td>
<td>0.0003</td>
<td>16</td>
<td>0.1 % R mode 0.04% C Mode</td>
</tr>
</tbody>
</table>
conductive trace on body, that is needed for both of the targeted applications, electric paint has been used. Electric paint is a nontoxic conductive substance which is water soluble. It has low resistance, so it is suitable to be used as a conductive material in electric experiments. In this design, the electric paint is used on filter paper made of cellulose fibers. These fibers are rough, therefore as electric paint is painted on to it, the soft ink gets absorbed and adheres to the paper, making it a nice, conductive electric trace (Fig. 3.13).

The electrical resistance of the conductive trace, which is 5 mm in width, was measured and recorded at various lengths. According to the results, the conductive paint has a small resistance (50 Ω), and the resistance increases linearly with longer traces. The trace is not sensitive to slight bending, making it a good material to wear as electrode. Since the goal is to have an electrode, two paths were drawn on the filter paper. These paths are connected to the skin on top of the lungs with conductive wires. It must be noted that the intention was to use the electric paint on the skin as electrodes, however despite the initial advertisement of the company producing these paint, applying the paint directly on skin is not FDA approved. Based-on this inquiry, the paint is safe on body and it’s only a matter of time before using conductive paint as an electrode is normal.

For human subject experiments, a PCB was then fabricated using Express PCB, which is illustrated in Fig. 3.14. The system depicted can be connected to the chest for trans-thoracic impedance measurement, Fig. 3.15, as the first application. This system is a 10g trans-thoracic impedance measurement system that is adhered to the chest using medical tape and facilitates low impedance connection to skin with electrical paint. The hand gesture recognition system (the second application) is developed using adhesive copper tape, with 16 1cm×1cm electrodes made on a Velcro strap. Fig. 3.16 shows the system on wrist. To reduce the error, the same size of electric paint is put on the wrist. The Fabricated PCB uses a Coin battery to power up the whole system, and a MAX 863DS, a Dual, High-Efficiency, DC-DC Controller is used to supply the chip voltage. MAX 863DS is cheap and can supply adjustable voltage as low as 1 V using 2 feedback resistors marked on the PCB as FB1 and FB2. Another advantage of MAX 863DS is its low-battery Output (LBO). An open-drain N-channel MOSFET output that is connected to ground when the voltage on Low-Battery comparator input (LBI) drops below 1.25 V. To use this function LBI pin is set on 1.25 V,
Figure 3.13: Bare conductive paint is used to (a) draw electrodes on filter paper, (b) the electrodes are then cut, the wire put on the paint, and (c) put on skin with the system using medical tape to measure the impedance.
therefore when the battery voltage drops lower than 1.25 V, LBO is connected to ground. A low power SMD LED is connected to this pin, in series with a resistor and connected to a battery so that it indicates the need to change the battery when it turns on.

In order to transfer the output signal for further remote processing, the Quasar UK FM hybrid transmitter module is used. The module is very simple to set up, does not need additional parts to operate, and offers low current consumption (typ. 1mA). Data can be supplied directly from CMOS/TTL devices and has a low hardware cost ($6). The low current consumption, allows for extended battery life when used in mobile applications. The FM transmitter is depicted in Fig. 3.14 and the receiver block can be seen in Fig. 3.17. In comparison to RF module used in [100, 101], this RF transmitter uses 10 times less power, is smaller, and does not require a micro-controller to send or data. The receiver system is flexible to set up. In this test, the receiver was connected to an Arduino board and the received data was communicated to a laptop through serial communication. The Arduino
is used primarily for ease of use in connecting the receiver to the laptop. The signal is then modulated and sent by the transmitter. The transmitter was tested both with 30 cm and 1.5 m distance from the receiver, with no degradation of signal. The last stage of this circuit is an SR-latch that changes the pulse width to a high frequency pulse train. The pulse width associated with the resistance or capacitance measured is coded in the number of pulses. Since this data is coded to the number of pulses, receiver delay or the change of signal amplitude from chip level (1.8 V) to TTL (3 V) during transmission cause no problem.

For human subject experiment, the recruitment and testing complied with IRB code of conduct. All the participants read and signed a consent form before entering the study. They were explained the process and could stop participating at any time. For the thoracic impedance measurement, a male and female subject were tested. For the hand gesture recognition, the system was tested on one female subject.

**Thoracic Impedance**: The system was tested on a male and a female to prove the measurement remains constant in time for a healthy person. The signal is measured and calculated for 5 times in a 12 hours period, and the average impedance and standard deviation are shown in Table. 3.3.
Hand Gesture: The hand gesture recognition system was stabilized on the wrist using adjustable Velcro tape. The 16 electrode and conductive paint dots on the wrist were placed, and a stimulating signal was applied to each electrode pair. The impedance on the other electrode was then measured. The experiment was repeated 4 times for each gesture and 5 different gestures. The results are shown in Fig. 3.18. When doing the experiment, the stimulating 40kHz sinusoidal signal is applied through two electrodes. For measurement, the electrode adjacent to the stimulating electrode is ignored, and all the other pairs are measured giving 13 measurements. In Fig. 3.18 (a) the results are shown in a heat map for letters A-D shown in sign language. For this experiment, the stimulation electrode is placed on the palm side, in middle of the wrist where main tendons lies. For a better presentation, impedance ratio to relax is shown in the figure, the impedance for relax position is therefore one, and all the other impedances are compared to the relax position. It is observed that electrodes that are placed on the bone have a slighter change in different hand gestures. Fig. 3.18 (b) shows the pattern of impedance measured for different hand gestures. This data measurement is proof of concept that with data processing along with a simple predicting algorithm, gestures of sign language can be detected with a device with 30µW power consumption.
Figure 3.18: Hand gesture recognition results showing the impedance of sign language letter A-D. The impedance is measured in ratio to relax status in (a) heat map (b) line plot.

3.3 Conclusion

In recent years the use of CMOS technology has single-handedly pushed many biomedical wearables, implantable and wireless devices to progress. Among these, use of digital output devices with frequency modulation is more favorable due to noise immunity in frequency/time modulation data transfer. A quasi digital output design combines the benefit of analog devices (low power, less complexity) and digital devices, to generate a pulse, frequency/time base output using analog blocks [102]. For this impedance sensor current and voltage comparators are used for simultaneous measurement of resistance and capacitance. The design does not use multiple switches or current sink/sources to enable low power function of the system.
Table 3.3: Human experiments done 5 times in a day every 3 hours showing measured resistance, capacitance and standard deviation.

<table>
<thead>
<tr>
<th></th>
<th>Resistance (Ω)</th>
<th>Deviation (Ω)</th>
<th>Capacitance (nF)</th>
<th>Deviation (nF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male Subject</td>
<td>114</td>
<td>115</td>
<td>112</td>
<td>1.2</td>
</tr>
<tr>
<td></td>
<td>114</td>
<td>114</td>
<td>112</td>
<td>1.2</td>
</tr>
<tr>
<td>Female Subject</td>
<td>100</td>
<td>104</td>
<td>101</td>
<td>1.6</td>
</tr>
<tr>
<td></td>
<td>101</td>
<td>104</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The impedance sensor design consumes an average power of 16µA using 1.5 V power supply and area of 300 µm². Experimental results show that the design is capable of detecting biological impedance with reasonable accuracy and sensitivity and has been implemented in 180 nm CMOS technology. Assuming mass fabrication for chip and PCB, the whole system costs under 10$ and consumes 3 mW including the RF transmitter. Using a 3 V coin battery, the system can work for up to 140 hours without the need for standby mode or a pause in impedance sensing. The system weighs 10 grams and is 4.5 cm × 2.5 cm big, making it suitable for connection to body using an adhesive medical tape without the need for any kind of strapping. The functionality of system is tested with conductive paint on filter paper for accuracy. With the advancement of conductive paints in near future, the use of the system is possible without the need for medical electrodes and contact gels.
Chapter 4

Temperature Sensor

Portions of this document were previously published in
“A sub-μW CMOS temperature to frequency sensor for implantable devices.”


4.1 Design

The first version of the circuit is shown in Fig. 4.1, where PTAT signal is converted to temperature through a scaling transistor and current mirror, and then finally charges a capacitor. A comparator controls a switch, which allows the capacitor to discharge once the voltage reaches the reference voltage. The resultant temperature is frequency-modulated for transmission. Since analog to digital conversion modules are typically power hungry, eliminating them and using direct frequency conversion significantly reduces the power consumption. This version however, was less accurate since it depended on natural discharging of the capacitor. The output was sinusoidal like signals that were hard for a digital block to detect. The 3 transistor temperature reference is inspired by [103] here. In this circuit bias current is provided by a reverse biased diode composed by gate source
Figure 4.1: Frequency based temperature sensing system with a single comparator.

connected transistor (TN₆), and TN₇ and TN₈ form the structure that provide the reference voltage by providing the difference between their gate-source voltages.

The circuit schematic of the final presented temperature to frequency converter sensor is shown in Fig. 4.2. It consists of a PTAT generation circuit, consisting of T₁-T₄, opamps, current mirror, a capacitor getting charged, and discharged by the output of the SR latch, comparators, and the reference circuits for the two voltages, Ref₉H and Ref₉low.

The design is implemented with Weak Inversion MOS PTAT generator. \( V_{PTAT} \) is the voltage proportional to absolute temperature (Fig. 4.2). The implemented circuit achieves both low voltage and low power operation. T₁, T₃ provide proper biasing for T₂, T₄. The drain current is given by,

\[
I_{sub} = \mu C_{OX} \frac{W}{L} V_{T}^2 e^{\left(\frac{V_{gs}-V_{th}}{nV_{T}}\right)} \left[1 - e^{\left(-\frac{V_{ds}}{V_{T}}\right)}\right]
\]

(4.1)

where \( \mu \) is the mobility, \( C_{ox} \) is the oxide capacitance, \( V_{T} \) is the thermal voltage, \( W/L \) is the aspect ratio of the transistors, \( V_{gs} \) is gate to source voltage, \( V_{ds} \) is the drain to source voltage, \( n \) is the subthreshold slope, and \( V_{th} \) is the transistor threshold voltage. If \( V_{ds} > 3V_{T} \) which is about 75 mV at room temperature, 4.1 can be reduced to,

\[
I_{sub} \approx \mu C_{OX} \frac{W}{L} V_{T}^2 e^{\left(\frac{V_{gs}-V_{th}}{nV_{T}}\right)}
\]

(4.2)

By putting the current that goes through T₂ and T₄ equal, \( V_{PTAT} \) can be calculated. In the following equation \( V₁ \) is the connecting point of biasing stage and \( V_{PTAT} \),
Figure 4.2: Final frequency based temperature sensing system using weak inversion MOSFETs.

\[
\mu C_{OX} \frac{W}{L} V_T^2 e^{\left(\frac{V_1-V_{PTAT}-V_{th2}}{nV_T}\right)} \approx \mu C_{OX} \frac{W}{L} V_T^2 e^{\left(\frac{V_1-V_{th4}}{nV_T}\right)} \left[1 - e^{\left(-\frac{V_{PTAT}}{V_T}\right)}\right] \quad (4.3)
\]

With further simplification,

\[
V_{PTAT} + nV_T \ln\left(1 - e^{\left(-\frac{V_{PTAT}}{V_T}\right)}\right) \approx nV_T \ln\left(\frac{W/L}{(W/L)_4}\right) - \Delta V_{th2,4} \quad (4.4)
\]

Where \(\Delta V_{th2,4}\) is the difference of threshold voltages due to body effect. To simplify the theory, body effect is ignored. The PTAT voltage is given by,

\[
V_{PTAT} \approx U_T n \ln\left(\frac{W_2/L_2}{W_4/L_4}\right) + U_T W \left(n e^{-n \ln\left(\frac{W_2/L_2}{W_4/L_4}\right)}\right) \quad (4.5)
\]

where \(U_T\) is the thermal voltage, \(W/L\) is the transistor aspect ration, and \(W\) is the Lambert W function, defined as the inverse of \(f(W) = W e^W\). \(V_{PTAT}\) has positive temperature dependence if \(T_2\) is larger than \(T_4\). The Lambert function is a mathematical construct to aid the solution of exponential equations and can be found in widely available comprehensive mathematical formulae books.

The resultant PTAT voltage achieves good linear relation between PTAT voltage and temperature over 0 °C to 50 °C temperature range. By changing the aspect ratio of the PTAT transistors, the output temperature dependencies can be adjusted. By feeding the PTAT signal to an amplifier and a scaling transistor, this voltage based signal is converted to current. The output current then goes through a current mirror and charges the capacitor.
Table 4.1: Transistor sizes for 130nm 8rf temperature sensor chip

<table>
<thead>
<tr>
<th>Converter</th>
<th>W/L</th>
<th>Comparator</th>
<th>W/L</th>
<th>Latch</th>
<th>W/L</th>
</tr>
</thead>
<tbody>
<tr>
<td>T_1</td>
<td>0.28/0.12</td>
<td>T_{11},T_{14}</td>
<td>1/0.21</td>
<td>T_{C8},T_{C9}</td>
<td>0.3/14</td>
</tr>
<tr>
<td>T_2</td>
<td>20/2.88</td>
<td>T_{12},T_{13}</td>
<td>0.5/3</td>
<td>T_{C10},T_{C13}</td>
<td>0.3/7</td>
</tr>
<tr>
<td>T_3</td>
<td>0.16/0.12</td>
<td>T_{C1}</td>
<td>0.3/7</td>
<td>T_{C14},T_{C17}</td>
<td>0.3/28</td>
</tr>
<tr>
<td>T_4</td>
<td>0.2/40</td>
<td>T_{C2}</td>
<td>0.6/7</td>
<td>T_{C18}</td>
<td>0.3/4</td>
</tr>
<tr>
<td>T_5-T_7</td>
<td>0.7/3</td>
<td>T_{C3},T_{C4}</td>
<td>1.2/7</td>
<td>T_{C19},T_{C20}</td>
<td>0.3/7</td>
</tr>
<tr>
<td>T_8-T_9</td>
<td>0.5/3</td>
<td>T_{C5},T_{C6}</td>
<td>4/7</td>
<td>T_{L1},T_{L4}</td>
<td>0.22/7</td>
</tr>
<tr>
<td>T_{10}-T_{15}</td>
<td>45/25</td>
<td>T_{C7}</td>
<td>0.3/7</td>
<td>T_{L5},T_{L8}</td>
<td>0.8/7</td>
</tr>
</tbody>
</table>

A cross-coupled latch comparator is used to ensure a fast comparison of inputs with a low power supply. Based on $V_{PTAT}$, CT is charged and discharged. The charging and discharging rate results in a temperature proportional to frequency. The two comparator references are shown as $Ref_{High}$ and $Ref_{Low}$. These two reference voltage, based on [103], are supplied by a 3-transistor, self-cascode. The circuit uses body effect induced threshold voltage variation and a reverse biased diode, making the circuit a temperature compensated voltage reference. The references are extremely low power, using 65.8 pW at room temperature. The voltage reference temperature variation is 22 ppm/°C and 34 ppm/°C for the high and low voltage reference, respectively.

The current $I_{charge}$ drives the capacitor, CT, between $Ref_{High}$ and $Ref_{Low}$. When $V_{CT}$ decreases to $Ref_{low}$, the SR latch resets, applying a digital low to TN1, leading to charging of the capacitor. By $V_{CT}$ increasing over $Ref_{High}$, the SR latch sets Q to high, starting the capacitor discharge phase. Charging and discharging of this capacitor continues leading to an oscillation frequency. This frequency can be a good measure of the temperature since it’s inversely proportional to the temperature and directly proportional to the current.

**Comparator and latch**: The transistor sizes for the designed comparator are given in Table 4.1 as $T_C$. The comparator is a standard design, with 3 stages. The first stage, pre-amplification is a differential amplifier. The next stage, cross coupled decision circuit with hysteresis, decides whether the output should be high or low based on the amplified input signal. The third stage is the output buffer. The amplifier is an ultra-low power
Table 4.2: Transistor sizes for 180nm temperature sensor chip

<table>
<thead>
<tr>
<th>Converter</th>
<th>W/L</th>
<th>Converter</th>
<th>W/L</th>
</tr>
</thead>
<tbody>
<tr>
<td>TN_1</td>
<td>2/0.18</td>
<td>TN_8</td>
<td>1/0.21</td>
</tr>
<tr>
<td>TN_2</td>
<td>50/1.44</td>
<td>TN_9</td>
<td>0.5/3</td>
</tr>
<tr>
<td>TN_3</td>
<td>64/0.36</td>
<td>TP_1, TP_2</td>
<td>1/3</td>
</tr>
<tr>
<td>TN_4</td>
<td>20/1.44</td>
<td>TP_3</td>
<td>1/3</td>
</tr>
<tr>
<td>TN_5</td>
<td>0.5/3</td>
<td>TA_1-TA_2</td>
<td>1.2/7</td>
</tr>
<tr>
<td>TN_6</td>
<td>25/1</td>
<td>TA_3-TA_4</td>
<td>4/7</td>
</tr>
<tr>
<td>TN_7</td>
<td>45/25</td>
<td>TA_5-TA_6</td>
<td>0.3/7</td>
</tr>
</tbody>
</table>

differential amplifier with power consumption of 69 nW, and is designed with 5 transistors. The design optimizes the minimum area, making it suitable for compact applications. A CMOS NAND gate based SR Latch is used as the output stage of the temperature sensing system. Transistors are sized to work in ultra-low power regime of 3nW, and sizes shown in Table 4.1 as T_L. T_{L1}-T_{L4} are PMOS transistors. NMOS transistors are T_{L5}-T_{L8}. Each nor gate has an input terminal cross-couple to the output of the other NOR gate. The latch is fast to be compatible with frequencies as high as 100 kHz and has a full rail swing. The sizes for 180nm Temperature sensing chip is shown in 4.2. The comparator consists of a standard input preamplifier and decision circuit. The pre-amplifier stage is the similar to the amplifier designed above. The circuit uses positive feedback from the cross-gate connection of TC_7 - TC_{10} to increase gain of the decision element. TC_7 - TC_{10} width to length ratio are 0.4/7 (µm/µm). The comparator power consumption is 69 nW.

4.2 Simulation and Experimental Results

In this section, the data for the standalone temperature sensor is measured through simulation and experiment. The first design of temperature to time frequency was implemented in 180 nm. Simulation in Fig. 4.3 shows the output frequency variation for a temperature change from 0 °C to 50 °C in steps of 0.5 °C is shown . The maximum frequency deviation obtained from simulation is 150 Hz, corresponding to an accuracy of 0.2
\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{fig4_3.png}
\caption{Output frequency variation for temperature change of 0 \textdegree C to 50 \textdegree C in steps of 0.5 \textdegree C for 180 nm temperature sensor.}
\end{figure}

\begin{quote}
\textbf{Figure 4.3:} Output frequency variation for temperature change of 0 \textdegree C to 50 \textdegree C in steps of 0.5 \textdegree C for 180 nm temperature sensor.
\end{quote}

\degree C. There is total 38 kHz frequency change over the 0 \textdegree C to 50 \textdegree C range. This corresponds to a frequency change of 760 Hz per 1\textdegree C. The deviation of the output frequency as a function of temperature from a linear best fit line gives the smallest detectable frequency change as 150 Hz. Thus, the resolution is 0.2 \textdegree C. The temperature sensor output at three 3 different temperatures, 0 \textdegree C, 25 \textdegree C, and 50 \textdegree C, is 11.82 kHz, 27.72 KHz, and 50.23kHz and is shown in Fig. 4.4. All three signals are large enough to be detected without the need for another amplifier.

The second design of temperature to time sensor was fabricated in a standard 130 nm process. This CMOS process offers up to 8 metal layers with a single poly layer. Supply voltages for this fabrication process are 1.2 V core and 3.3 V I/O. For the simulation results output of the temperature sensor was measured for 3 different temperatures to make sure the output has a Quasi-digital form. As seen in Fig.4.5, the output of the SR-latch is large enough to be transmitted. To check on process and variation effect on the linearity of the temperature sensing system Monte Carlo simulation is performed at 27\textdegree C on five process corners using 200 runs. In Fig. 4.6 different temperatures of Monte Carlo simulation is shown as distribution of frequency. At each temperature, an independent Monte Carlo simulation is performed, and the scatter plot of the frequency for each temperature is plotted. Since \(V_{PTAT}\) is larger at higher temperatures, the output frequency has larger spread at the higher temperatures. The mean of frequency is 51 kHz, 65 kHz, and 83 kHz for 0\textdegree C, 25\textdegree C and 50\textdegree C, respectively and the mean deviation is approximately 10kHz for the mentioned temperature.
The first experimental measurement was $V_{PTAT}$, measured for temperatures from 25°C to 150°C. This temperature range corresponded to a linear change from 47 mV to 62 mV for $V_{PTAT}$ (Fig. 4.7). This voltage is amplified deferentially and converted to current to have a good sensitivity considering the small voltage range (range in mV). The temperature associated voltage was measure once while heating the chip and the second time while cooling the chip to ensure there is no hysteresis in the temperature sensing. The comparator has also been tested experimentally by applying a sinusoidal voltage to (Input+), and a DC voltage applied to the negative input (Input-). The output of the comparator is shown in Fig. 4.8. With the change in Input- and Input+ will translate into a rail to rail output voltage. The experimental test was done on 4 different chips to confirm the results. To improve the system accuracy, a large comparison window is proposed using a low switching voltage (0.1 V). To increase the system speed and decrease the occupied area, a small capacitor is used.

The system setup for measuring temperature to voltage is shown in Fig. 4.9. To set the ambient temperature, a temperature chamber is used. The temperature chamber has
Figure 4.5: Frequency output signal at 0, 25, and 50 °C for 130nm technology temperature sensor.

Figure 4.6: Distribution of frequency output over the temperature range 0 °C to 50 °C for 130 nm technology temperature sensor.
Figure 4.7: Output voltage as a function of temperature for 25 °C to 150 °C for chip fabricated in 130 nm CMOS technology.

Figure 4.8: Experimental verification of the comparator for chip fabricated in 130 nm technology.

the ability to change the temperature in controllable increments; in this experiment the temperature was changed for 25 °C to 75 °C in 2.5 °C increments. The pulse width of the output signal is measured for each temperature. The chip was then cooled down to 25 °C again, and the output pulse width associated with the temperature was measured in the same increments. The chamber test experimental result is shown in Fig. 4.10. The results illustrated in this figure shows that the temperature is linear up to 60 °C, and then the slope changes slightly. Since the PTAT generation is fairly linear, the non-linearity is associated
Figure 4.9: Experimental setup for temperature to time sensor using a temperature chamber.

Figure 4.10: Experimental measurements of temperature to time sensor using a temperature chamber for chip fabricated in 130 nm technology.

with voltage to time conversion. All three signals are large enough to be detected without the need for further additional amplification. Fig. 4.11 shows the input referred noise is 85 \( \mu V/\sqrt{Hz} \) at 10 kHz for the temperature range.

The comparison of the sensor to state of art is shown in Table. 4.3 as Sensor 2. Sensor 1 is the previous work of this author published in [104]. The article uses a similar method.
to design an ultra-low power temperature sensor for integration into implantable devices. The previous sensor however, does not have a window comparator scheme and relies on the natural discharge of a capacitor to ground to reset the system, which reduces the accuracy and resolution of the system. In the new sensor, the transistors are also better scaled in sub-threshold region to reduce the power consumption of the system.

4.3 Conclusion

In this section state of art quasi-digital temperature sensor is developed. The temperature sensor enables low power consumption and low area for portable and miniaturized applications. The sensor uses a proportional to absolute temperature (PTAT) voltage generation circuit. The sub-\(\mu\)W temperature sensor uses sub-threshold transistors and nW 3-transistor voltage references to change PTAT voltage to frequency. The temperature sensing system for the temperature range of 0 °C to 50 °C is implemented in a 130 nm process. The power consumption of the overall system is 195 nW, with 0.5 V supply voltage. The overall area is 0.008 mm\(^2\), including the voltage to frequency conversion that eliminates the need for ADCs and external clocks. One of the main shortcomings of all of these integrated circuits is the lack of security. No means of security is directly incorporated on-chip, however, when

Figure 4.11: Noise spectral density at 10 kHz over the operational temperature range for chip fabricated in 130 nm technology.
transmitting data, privacy and secrecy of sensitive information seem crucial. Security is even more critical when dealing with biomedical devices.
Chapter 5

Hardware Security

Portions of this chapter are published in


Emerging CMOS applications are imposing higher performance and efficiency requirements on the hardware. One of these new requirements is the existence of security in circuits with data transmission. Hardware integrated security is one means of implementing security on-chip. This method, code the signal from the start, eliminating the source of threat to your privacy. Using Chaotic circuits is a method of ciphering communication in IoT devices. These ciphering systems (here implemented as chaotic shift-keying) can be fabricated using CMOS technology as a single chip. The backbone of these ciphering systems, chaotic systems, each with different starting initial conditions generates a ciphered signal. Because of the exponential divergence of the nearby trajectories of chaotic systems,
matching of these systems used as a transmitter and receiver may seem surprising. This matching is one amazing characteristic of the chaotic system called synchronization. When two chaotic systems share a common state, synchronization of chaos happens.

This section demonstrates the implementation of integrating analog security with sensors and takes the initial step towards having hardware-based integrated security encryption in any IoT and arrayed sensor systems. In this work, presented in section 4, a temperature sensor with frequency output is designed using sub-threshold Mosfets as the sensing system. The other sensor presented in section 3 is a comparator based current to frequency conversion [102, 104]. In this chapter, a chaotic transmitter/receiver encryption system based on [107] is inspected from a security point of view and integrated with the sensors. The developed transmitter/receiver is the first to eliminate attacks using a time scaling parameter. The system is developed by improving the design and experimentally demonstrating the encryption algorithm with a complete low power temperature sensor. The system is the first experimentally demonstrated CMOS temperature sensor with printed circuit board that implements the Lorenz-based chaotic encryption/decryption system to the authors’ knowledge. Then an on-chip integration of Lorenz chaotic circuit is implemented in 180 nm technology. In this section, each design and a full secure sensor system that can be fabricated on a single chip is presented. The base of this design is Lorentz equations, which is implemented using modular building blocks (Integrator, Multiplier, Amplifier).

5.1 Design

Encryption is an information encoding process that prevents reading and understanding of information by unauthorized parties. There are many counter-attacks for encryption; in one method, the attacker can use cryptanalysis to decode the encryption and translate the information. Using computers, fast and cheap encryption has become possible. However, it has also given attackers the necessary tools to allow brute force methods of code-cracking. The goal of both asymmetric and symmetric ciphers is to combat third party attack [107].

Chaotic encryption is an encryption method that utilizes Chaotic Shift Keying (CSK). It masks data through a chaotic system that is very sensitive to initial conditions and system
parameters. It is a nonlinear system and allows encryption over bit-wise signals. This type of encryption is suitable for portable, wireless sensors that use a digital output to convey information. Private and secure communications is a very high priority, especially in the modern tech era. Because of this, cryptography is becoming increasingly popular. Cryptography and code-breaking have been used since near the beginning of documented human history [107, 108]. Today, computers have made automatic encryption inexpensive, but have also improved code-cracking capabilities. Here chaos synchronization of two Lorenz systems is used to cipher analog signals.

### 5.1.1 Mathematical Realization

Two chaotic systems that have different starting initial conditions, even with a minimal difference in their initial condition, seem impossible to match because of the exponential divergence of the nearby trajectories. Though surprising, when the two systems are coupled with a single shared state provided by the drive system, it can exhibit a phenomenon known as Synchronization of Chaos [109]. The second system is known as the driven system, in this case, the receiver. However, many previous designs have proven to limit the success of synchronization on how well the system parameters are matched.

The chaotic nature and possibility of synchronization of these systems make them perfect candidates to make encryption masks. As an example, this method has been successfully used in speech applications. However, the theory places various limitations on the kind of data that can be successfully encrypted and securely communicated between two systems [110]. Chaos using a Lorenz system and Chua’s circuit are among promising systems, in theory, to use for masking of binary systems [111, 112]. This method, known as chaotic shift keying (CSK) uses the chaotic signal as a carrier for information.

The Lorenz based CSK system is described by (5.1),

\[
\begin{align*}
\dot{x}_1 &= \sigma(x_2 - x_1) \\
\dot{z}_1 &= \sigma(z_2 - z_1) \\
\dot{x}_2 &= (\beta(m) - x_3)x_1 - x_2 \\
\dot{z}_2 &= (\beta(m) - z_3)x_1 - z_2 \\
\dot{x}_3 &= x_1x_2 - \rho x_3 \\
\dot{z}_3 &= x_1z_2 - \rho z_3
\end{align*}
\]
The system states $x_1$, $x_2$, and $x_3$ describes the system which is performing the driving, in this case transmitting function. For the driven or receiver the systems states are named $z_1$, $z_2$, and $z_3$. $\sigma$ is Prandtl’s number. $\beta(m)$ is given by,

$$\beta(m) = \begin{cases} 
\beta_0 & \text{if } m = 0 \\
\beta_1 & \text{if } m = 1 
\end{cases} \quad (5.2)$$

$\beta(m)$ is a binary variable gain parameter generating the binary signal $m$. $\beta_0$ and $\beta_1$ are different enough to diminish noise and parameter uncertainty extraction errors. However, these two parameters are still within some tolerance value. This tolerance limit should not affect the transmitted state signal characteristics. The synchronization error, $\Phi_{sync}$, is,

$$\Phi_{sync} = \begin{bmatrix} 
\Phi_1 \\
\Phi_2 \\
\Phi_3 
\end{bmatrix} \quad (5.3)$$

$$\Phi_1 = x_1 - z_1$$

$$\Phi_2 = x_2 - z_2$$

$$\Phi_3 = x_3 - z_3$$

For $m = 0$, the derivative with respect to time of the error states synchronization are,

$$\dot{\Phi}_1 = \dot{x}_1 - \dot{z}_1 = \sigma(\Phi_2 - \Phi_1)$$

$$\dot{\Phi}_2 = \dot{x}_2 - \dot{z}_2 = -(x_2 - z_2) - (x_3 - z_3)x_1 = -\Phi_3x_1 - \Phi_2 \quad (5.4)$$

$$\dot{\Phi}_3 = \dot{x}_3 - \dot{z}_3 = (x_2 - z_2)x_1 - \rho(x_3 - z_3) = \Phi_2x_1 - \rho\Phi_3$$

$V(\Phi)$ is a Lyapunov function. This function is chosen, based on [111] to demonstrate stable asymptotic synchronization error $\Phi_{sync}$ when the message $m = 0$,

$$V(\Phi) = \frac{1}{\sigma}\Phi_1^2 + \frac{1}{\sigma}\Phi_2^2 + \frac{1}{\sigma}\Phi_3^2$$

$$\dot{V}(\Phi) = \frac{2}{\sigma}\dot{\Phi}_1\Phi_1 + \dot{\Phi}_2\Phi_2 + \dot{\Phi}_3\Phi_3 = -\Phi_1^2 - \Phi_2^2 - \rho\Phi_3^2 \quad (5.5)$$
For \( m = 0 \), it can be seen that global asymptotic stability can be demonstrated. In equation (5.5), \( V(\Phi) \) is positive definite and radially unbound. \( \dot{V}(\Phi) \) is negative definite. Furthermore, it can be shown that for \( m = 1 \), synchronization error’s derivative with respect to time is,

\[
\begin{align*}
\dot{\Phi}_1 &= \sigma(\Phi_2 - \Phi_1) \\
\dot{\Phi}_2 &= \dot{x}_2 - \dot{z}_2 = (\beta_\Delta - \Phi_3)x_1 - \Phi_2 \\
\dot{\Phi}_3 &= \Phi_2x_1 - \rho\Phi_3
\end{align*}
\]

(5.6)

where,

\[
\beta_\Delta = \beta_1 - \beta_0
\]

(5.7)

From equation (5.6), the coordinate at which synchronization occurs, \( \Phi_{\text{sync}} = [0 \ 0 \ 0]^t \), does not reflect a system equilibrium. This creates a mismatch in synchronization resulting in an error relative to the message, \( m \).

To implement the aforementioned mathematical equations, common analog circuits, such as resistors, capacitors, comparators, and operational amplifiers, can be used. This accomplishes low power signal processing compared to having a micro-controller to implement these equations. Thus, the dynamic chaotic encryption techniques, can be implemented using electronics. No commercial CSK encryption technology is currently available for widespread use. There has been some limited implementation in circuits, mostly discrete or using FPGAs however, these devices are not viable options for current low power applications and as explained in 5.1.2 the CSK system is probably not secure on its own [108].

5.1.2 The Return Map Attack

As security advances, attackers also come up with techniques that can be used to defeat CSK encryptions methods, Return Map (RM) attack is one of these techniques where a local extrema is observed to determine the time varying features of the system [113]. This method depends on the presumption that the symmetric nature of the Lorenz system will
push a dynamic return map towards a one-dimensional set. This one-dimensional data can be developed by examining a single state.

To achieve this, the return map from the \( n_{th} \) local extrema (maxima and minima) of the initial or secondary state of equation (5.1), is written as \( \bar{X}_n \) and \( \bar{Y}_n \) respectively. A comparison of functions makes up the developed return map, and is,

\[
\begin{align*}
A_n &= \bar{X}_n + \bar{Y}_n \\
B_n &= \bar{X}_n - \bar{Y}_n
\end{align*}
\tag{5.8}
\]

A plot of \( A_n \) as a function of \( B_n \) yields the three line return map. The map is implemented by correlation of the local extrema to the focal point. From the output state of \( x \), the map is then determined, using the CSK encryption methodology results in a map shown in Fig. 5.1.

The CSK method previously introduced will always be vulnerable to the return map attack since in this method the signal is directly generated by modulation of system parameters \( \beta \) or \( \rho \) for data encryption. The CSK technique modulates the focal point depending on a bit being present or absent. This leads to the return map vulnerability due to significant distortion in the system dynamics [114].

### 5.1.3 Return Time Map Attack

To diminish the vulnerability of system to a return map attack, time-scaling encryption modulation can be introduced in this system. To defeat an RM attack easily, encryption
modulation using a time-scaling factor needs to be performed. In this method, a time scaling factor on maxima and the time window between maxima of the transmitted signal can be used [115]. An example of RTM on a signal with a time-scaling factor and only one switching event is shown in Fig. 5.2. In this figure, a return time map attack is not required since the changing bit is detected by searching for significant changes in the transmitted state. However, as Fig. 5.2 shows, an RTM can detect the error when simple false switching events occur.

5.1.4 Time Scaling Chaotic Shift Keying

vulnerability of CSK security system to return map attacks can be weaken using a "time scaling function", \( \lambda(x(t), m) \) to encrypt the signal, \( m(t) \). For any autonomous dynamical system,

\[
\frac{d}{dt} x = f(x)
\]  \hspace{1cm} (5.9)

where the time scaling function is defined by,
\[
\frac{dt}{d\tau} = \lambda(x) \\
\tau(t_0) = \tau_0 \\
0 < \lambda(x) < \infty
\] (5.10)

It is clear that then,

\[
\frac{d}{d\tau} x = \lambda(x)f(x) 
\] (5.11)

From equation (5.10) \( \tau \), is strictly monotonic and increases with time, \( t \) [116]. From equation (5.11), the \( \lambda(x) \) does not alter the phase space of \( x \) with respect to its attractors or equilibrium. To have the synchronization of the two system intact, trajectory of \( x \) is not distorted by the time scaling factor. The only effect of adding \( \lambda(x) \) is change of time the system needs to complete or reach a stable value [108]. Encoding the message, \( m(t) \), with the time scaling factor can prevent the return map attack.

Using a function, \( \lambda(x,m) \), this time-scaling factor is applied to a Lorenz based chaotic system. By applying \( \lambda(x,m) \) to the system, a Time Scaling Chaotic Shift Keying (TS-CSK) encryption system is created. The system equations then become,

\[
\dot{x}_1 = \sigma(x_2 - x_3)\lambda(x, m) \\
\dot{z}_1 = \sigma(z_2 - z_1)\lambda(z, 0) \\
\dot{x}_2 = ((\beta(m) - x_3)x_1 - x_2)\lambda(x, m) \\
\dot{z}_2 = ((\beta(m) - z_3)x_1 - z_2)\lambda(z, 0) \\
\dot{x}_3 = (x_1x_2 - \rho x_3)\lambda(x, m) \\
\dot{z}_3 = (x_1z_2 - \rho z_3)\lambda(z, 0)
\] (5.12)

where,

\[
\lambda(x, m) = \begin{cases} 
\lambda_m & \text{if } \delta_x = 0 \\
\lambda_{1-m} & \text{if } \delta_x = 1 
\end{cases}
\] (5.13)
where $\delta(x)$ is the decision engine. Since security is the main consideration, the decision engine is chosen such that, the attacker can not decode or extract the switching event of $\lambda(x, m)$ from the signal that is being communicated. There are several options for ($x$) which satisfy these conditions. [108], uses $\delta(x)$ such that,

$$
\delta(x) = \begin{cases} 
0 & \text{if } \frac{v^T x}{h} \text{ is even} \\
1 & \text{if } \frac{v^T x}{h} \text{ is odd} 
\end{cases}
$$

where the unitary selection vector $v$ is,

$$
\Phi_{\text{sync}} = \begin{bmatrix} v_1 \\
v_2 \\
v_3 
\end{bmatrix}
$$

(5.15)

With higher frequencies of the Lorenz oscillation, the design and implementation of decision engine gets increasingly difficult and expensive. With these assumptions, the idea of simplifying the decision engine to two regions, the initial decision engine was designed.

$$
\delta(x) = \begin{cases} 
0 & v^T x < 0 \\
1 & v^T x \geq 0 
\end{cases}
$$

(5.16)

The decision engine described by equation 5.14 thwarts both types of return attacks (RM and RTM) [108]. Using the return map, the underlying Lorenz function does not change in correlation with the orbital foci, TS-CSK encryption therefore prevents the return map attack. Here, $x$, in the TS-CSK system of equation (5.12), is chosen so that the underlying Lorenz system is chaotic. The system is then protected from return map attacks. Return time map attacks require the message, $m(t)$ to somewhat hide the time difference between switching. To obfuscate $m(t)$, an even-odd scheme, with adequate number of switching occurring between bit changes can be used to prevent message extraction based on RTM [108]. This immunity however does not suffice for a plus-minus TS-CSK (PM TS-CSK) decision engines with a reasonable time difference between bits. A PM TS-CSK require a marginally more complicated decision engine. This is borne out the system equations,
\[
\delta(x) = \begin{cases} 
\delta_z & x_2(t) < -\sqrt{\rho(\beta - 1)} \\
1 - \delta_z & -\sqrt{\rho(\beta - 1)} \leq x_2(t) < 0 \\
\delta_z & 0 < x_2(t) < \sqrt{\rho(\beta - 1)} \\
1 - \delta_z & x_2(t) \geq \sqrt{\rho(\beta - 1)}
\end{cases}
\]  
(5.17)

where,
\[
\delta_z = \begin{cases} 
1 & x_3(t) \geq \beta - 1 \\
0 & x_3(t) < \beta - 1
\end{cases}
\]  
(5.18)

The regions of operation and switching of the system is derived from this new decision engine. Here, if the third dynamic, \(x_3(t)\), crosses from one side of its equilibrium to the other side, the system switches, regardless of the message. As an increase in regions of operation is favourable for an increased security, the system splits the second dynamic into 4 regions. These regions are are below the negative focus, between the negative focus and the origin, between the origin and the positive focus, and above the positive focus. Equations (5.17) and (5.18) describe the 8-section TS-CSK system. Using equations of the Lyapunov function, synchronization of the system, seen in equation (5.12), is described again (5.5). The error is the same \(\Phi_{sync}\) indicated in equation (5.3). The derivative with respect to time of \(\Phi_{sync}\) when the message \(m(t) = 0\) is,
\[
\dot{\Phi}_1 = \sigma(\lambda_x(x_2 - x_1) - \lambda_z(z_2 - z_1)) \\
\dot{\Phi}_2 = (\beta(\lambda_x - \lambda_z) + (\lambda_zz_3 - \lambda_xz_3))x_1 + \lambda_zz_2 - \lambda_xx_2 \\
\dot{\Phi}_3 = (\lambda_zx_2 - \lambda_xx_2)x_1 + \rho(\lambda_zz_3 - \lambda_zx_3)
\]  
(5.19)

An interesting case study is when the time scaling factor of the two systems are equal. This occurs when \(\lambda(x) = \lambda(z)\). When the message \(m(t) = 0\), this occurs for \(x\) and \(z\) within the same region of operation. Thus, \(\lambda(x) = \lambda(z)\), equation (5.19) reduces to an equation very similar to (5.4). The Lyapunov equation indicates asymptotic stability about the point \(\Phi_{sync} = [0 \ 0 \ 0]^T\). For both systems \(\lambda(x) \neq \lambda(z)\) is not always true. However, the chaotic system is cyclic. Additionally, the time-scaling factor does not change the phase space. Thus, the regions of \(\lambda(x) \neq \lambda(z)\) are periodic when no synchronization is occurring.
5.2 Practical System Realization

In this section the circuit implementation of the CSK system is presented. This system is described so far by the mathematical equations and shown in the block diagrams as the encryption transmitter (Fig. 5.3) and the receiver system (Fig. 5.4). The Gaussian noise here is the noise that corrupts the transmitted state $x_1$.

Using math equations $\beta_m$ module was implemented. The equation used was $\beta_m = (\beta_1 - \beta_0)m(t) + \beta_0$. Encoding of the message happens in modulation block. Transmitter and
Receiver block diagram of the TS-CSK communication system is shown in Fig. 5.5. The complexity and component number of the TS-CSK system has increased compared to the CSK system. The implementation of TS-CSK system using circuit component is shown in Fig. 5.7. The function $\lambda(x,m)$, described in 5.13, is implemented in both the transmitting and receiving module. The $\lambda$-modulation function is distributed inside the equations to be parallel to the CSK system. This distribution also eliminates the need for increased logic gates. The previous equation, (5.12), then becomes,

$$
\dot{q}_1 = \sigma(\lambda(q,m)q_2 - \lambda(q,m)q_1) \\
\dot{q}_2 = \beta g - gq_3 - \lambda(q,m)q_2 \\
\dot{q}_3 = gq_2 - \rho \lambda(q,m)q_3
$$

(5.20)

Where $g$ is chosen to be $\lambda(q,m)q_1$ or $\lambda(q,m)s$. This parameter is chosen based on the block being a transmitter or a receiver.

The first version of the circuit is a discrete version, based on the work of [107]. This original version was implemented using two boards, contributing to noise and mismatch. A new PCB combined the two boards and created a ground plane to reduce the noise and mismatch of the discrete implementation. In the fabrication of the board, the components were divided into two groups. The first group were the components getting the pulsed input and the second group were the components connected to the chaos outputs. The ground
signal in each of these groups were connected together and connected to each other at just one point. In this version of the circuits using discrete components, an LT1057 is used as the operational amplifier and an AD633 is used as the multiplier of choice. The DG419 handles the switching tasks.
The LT1057 was configured as a differential amplifier in order to extract $\Phi_{\text{sync}} = x_1 - z_1$. This is shown in Fig. 5.8. To remove the synchronization signal error that occurs due to difference in resistor and gain values, known as mismatch, anti parallel diodes are used. This error occurs in both transmitter and receiver systems.

5.3 Design and Results of Integrated Sensor with Discrete Chaotic Ciphering

To have a secure sensor, the chaotic security transmitter/receiver is tested with the temperature sensor Fig. 5.9. The main components of the encrypted low power temperature sensing system are the front end temperature sensor, a transmitter, and a receiver. The temperature sensor measures the temperature using a VPTAT block. After the conversion of VPTAT to frequency using quasi-digital temperature sensor, the signal is fed into a chaotic ciphering transmitter. The ciphered signal is then transmitted (using wire in this version and wireless transmission in the next versions) and the receive gets and decodes the signal without a third party having access to the transmitted data. The benefit of this system is secure transmission of analog data with a relative low power. Compared to implementation of security using software or micro-controllers this system can consumes much less power.

Next, the temperature sensor is integrated with the chaotic transmitter and receiver for analog encryption. Fig. 5.10 shows the test setup with the temperature sensor, transmitter, and receiver. The standalone temperature shows good linearity in generating VPTAT. Though some non-linearity was introduced in the temperature to time conversion, the system
still acted linear in the ranges up to 50°C which is the targeted range for wearable devices. The lid on the chip cavity of the fabricated temperature sensor is kept open to ensure the same temperature of the environment and integrated circuit. The transmitter and receiver along with the fabricated temperature sensor along with their connection, are seen in the picture. Voltage supplies are connected to the board, and the signals are seen using an oscilloscope (Fig. 5.10). Before the experiment on the chip and PCB, the ciphering of the signal is also done using Matlab Simulink.

To test the overall system, temperature sensor block output is fed to the signal transmitter. This signal shown in Fig. 5.11 (a) has a frequency proportional to temperature. The signal is coded in the transmitter shown in Fig. 5.11 (b). As illustrated the voltage level of the coded signal is not detectable at this point. This encoded signal is also not in phase with the input signal. To synchronize the two systems, one state of the transmitter and receiver are coupled. The transmitter sends the ciphered signal to the receiver. The signal at the input of the receiver is still, The encode signal Fig. 5.11 (b). Receiver then decodes the encrypted message. Fig. 5.11 (c) shows the decoded temperature data using Matlab Simulink, and Fig. 5.11 (d) shows the experimental decoded temperature data. Since the decode signal still carries the noise of the chaotic system, it is difficult to discern the actual pulses. Using an averaging or peak detection algorithm in Matlab tool boxes, the
temperature pulse can be extracted (Fig. 5.11 (e)). For integrated circuit implementation, at this step, a comparator can be used to recover the decoded digital temperature sensor signal by comparing it to a pre-determined threshold voltage.

5.4 Design and Results of On-chip Chaotic Ciphering

The first implementation of on-chip security was the Lorenz system depicted in Fig. 5.7. As seen in Fig. 5.7, the most important blocks of the designed block is integrator and multiplexer. Each circuit is designed and simulated separately. The integrator is based on [117]. It is a low power (µW) CMOS integrator implemented with an OTA and a capacitor whose time constant is large and tunable. The integrator is based on series block of $g_m - 1/g_m$. The application, matches the low power, low area goal since it was primarily designed to be used in an amplifier used in implantable systems. The integrator was employed to reduce unwanted artifacts. Four cascading stages are used. They consist of trans-conductance and resistance units, forming an attenuator, and an OTA driven capacitor. The attenuating section consists of two trans-conductance stages ($g_m$) interleaved with two $1/g_m$ stages. The
Figure 5.11: Experimental measurements. (a) $V_{PTAT}$ corresponding to 50°C temperature, sent to a transmitter to be encoded. (b) Voltage is encoded and sent as a secure signal. (c) Matlab simulink used to decode the secure sensor in simulation. (d) The experimental decoded temperature signal in the receiver. (e) Experimental temperature signal which is decoded in the receiver goes through optimization algorithms. Local peak detection to remove noise (solid line) and thresholding (dashed line) is used to optimize the signal.

$1/g_m$ act as resistances to ground. This section is an attenuator and is shown in Fig. 5.12 a. The output of the attenuator is connected to an OTA driving a capacitor C, as shown in Fig. 5.12 b section.

The OTA-capacitor section in Fig. 5.12 b. consists of a current source biasing p-type input amplifier. The current source biases the regulated cascode n-type mirrors, $M_5$ through $M_{10}$. Like all integrators, an integrating capacitor, shown by C, is connected across the high and low impedance output nodes. In an ideal circuit, the DC bias at the two capacitor nodes are identical for reduced DC offset when the output voltage ($V_O = V_{O1} - V_{O2}$) is taken
across the capacitor. Each $g_m$ stage of the attenuator was realized by a simple differential amplifier and each $1/g_m$ stage by a diode-connected n-channel transistor. Two $g_m$ and two $1/g_m$ stages were put in series. The extra diode-connected n type transistor, M11, in this design achieves improved DC operation. This diode is connected at the inverting input of the second OTA, as shown in Fig. 5.12 a.

For the multiplexer, many well known Gilbert cell typologies are used to multiply signals; however, most of these circuits are designed with BJTs. With advancement in fabrication technology and all designs going toward digital technology, analog circuits are required to be implemented in low-cost standard CMOS technology. Thus, the popular BJT Gilbert Cell is not suitable in a standard CMOS process, pushing designers toward designing in low power and low supply voltage requirements [118]. The logic behind the Gilbert cell design is to have a differential amplifier with a controllable output voltage. Multipliers implemented by
Gilbert cell is illustrated in Fig. 5.13. This design uses two resistive loads and eight NMOS transistors that are working in saturation region. The input signals are given in a differential manner. The inputs in this design are labeled in1 and in2 for the first differential input and in3 and in4 for the second one. Current sources in the picture provide the current needed to bias the circuit correctly. The top 4 transistors work as a switch that source the current in the lower part of the circuit. In the lower circuit, the signal is multiplied by the signal fed into $M_1 - M_4$, and the output obtained is a differential output.

In this design, multi-modal sensors output is chosen by a simple analog multiplexer and then fed to a chaotic transmitter for ciphering. The overall circuit diagram of the final design is shown in Fig. 5.14.

For the multiplexer, a very fast and compact, CMOS-based MUX device is built using two transmission gates, as shown in Fig. 5.15. In this design, the top transmission gate (with input ”a” connected to it) controls if the input from ”a” should pass to the output.
The "b" input operates similarly. The inverter is used to make sure that only one of the channels is selected (either input a or input b) and allowing the selected signal to pass.

To test the on-chip encryption circuit, first, the two main blocks of the system, the integrator and the multiplexer is tested. The integrator, and multiplier were fabricated using a 7 metal, single poly 0.13 nm technology. The fabricated chip is shown in Fig. 5.16. Using Cadence, simulations and layout was carried out. The chip is then fabricated using MOSIS fabrication service, and the blocks are experimentally tested. The integrator design is tested with a slow signal of 5 Hz and 20 mv to confirm the 1 s time constant. The integrator output voltage ($V_o$) response versus the input is shown in Fig. 5.17. Changing of the biasing current source can change $g_m$ and $i/g_m$ ratios leading to a change in time constant.

Transient analysis for the basic multiplier is done. The output is as shown in Fig. 5.18. As seen, the multiplication is applied to both the form and amplitude of the signal. Using
off-chip resistors, the system shown in Fig. 5.7 was setup. However, no oscillation was achieved due to the offset created due to the single-ended nature of circuit blocks. This lack of oscillation is seen in Fig. 5.19, As you can see the outputs of x and y correspond to each others value linearly. The offset mentioned here is formed at the output of single ended block. To eliminate this offset in discrete designs usually big capacitors in range of few 10 or few 100 $\mu$F is used, since this device is targeted for on-chip designs, no capacitors where used leading to offset of few mV in each cycle, driving the system to saturation. This offset is intrinsic in integrated devices because of the process variation and mismatch in device sizes.

In the next step, using the same blocks fabricated, a new fully differential on-time ciphering system shown in Fig. 5.20. Using differential scheme, the offset does not get
Figure 5.19: Single ended chaotic system showing no oscillation.

Figure 5.20: Fully differential on-time ciphering system.

aggregated, preventing the device to be derived in saturation. In case of implementing the
time scaling parameter, this block consisted of amplifier and transmission gates is connected
to output of integrator and then to the rest of the circuit. The output of the chaotic
ciphering circuit is simulated using a fully differential circuit instead of single-ended, and
the multiplexer and integrator. The simulation results shown in Fig. 5.21 shows the chaotic
behavior of the circuit.
The final security on-chip with replication of both impedance and temperature sensors along with a Lorentz ciphering transmitter is implemented in 180 nm. Receiving the chip, each block is first tested separately. The overall scheme of having a signal encoded by the transmitter and then sent and decoded by the receiver is presented here in experiment. The experimental result of the chaotic coded signal is shown in Fig. 5.22. The input of the system is the temperature signal (Fig. 5.22a). This signal is coded by the ciphering transmitter. This signal is then transmitted to the input of the receiver Fig. 5.22b. The signal seen in this stage is coded and a third party can not decode the message without having the exact circuit. Fig. 5.22c is the decoded signal at the output of the receiver.

The implementation of the transmitter and receiver on a prototype board is seen in Fig. 5.23. It must be noted that to be able to tweak the circuit, only one block from each chip is being used, however the whole circuit does fit on a 1.5mm×1.5mm chip based on the areas provided. In the picture the red wire is the first state of each block, connected for synchronization. Using this setup, getting the system to synchronize was challenging because of all the biasing resistor used. In my experiments, these resistors needed to be replaced by potentiometers to have slight changes in the biasing.

The designed chip is compared to the state of art in Table. 5.1. To have an easier comparison with the numerous design of systems implemented using electronic circuits for ciphering in communication, a figure of merit (FOM) is defined. Here the figure of merit

**Figure 5.21:** Simulation results of yz output showing chaotic behaviour of the circuit in 180 nm.
Figure 5.22: Experimental result of the coded and decoded signal by the ciphering transmitter and receiver implemented in 180 nm. (a) The temperature signal input to the transmitter, (b) the transmitter input and the receiver output, and (c) the decoded signal at the output of the receiver.
decrease as the systems get closer to a portable system. To define a figure of merit, the parameters that their decrease contributes to an improved system is gathered and these parameters are implement in terms of multiplying them. If a parameter improves the system by getting bigger, it is included in the figure of merit by division. To get to a number range easily comprehensible, the units are chosen, so the FOM ranges from thousands to one over thousands. To emphasize the importance of being robust to attacks, if the system is not robust to attacks, the FOM is multiplied by 10.

\[
FOM = Technology(\mu m) \times Area(mm^2) \times SupplyVoltage(V) \times Power(W) \times \\
\#ofblock \times TestSignalVoltage(V) \times TestSignalTime(s) \times AttackPrevention
\] (5.21)
Table 5.1: Comparison table with state of art chaotic communication.

<table>
<thead>
<tr>
<th>Year</th>
<th>Design</th>
<th>Area</th>
<th>Supply</th>
<th>Power</th>
<th>Test signal</th>
<th>Attack resistance</th>
<th>FOM</th>
</tr>
</thead>
<tbody>
<tr>
<td>[79]</td>
<td>1993</td>
<td>0.35µm</td>
<td>4mm²</td>
<td>±2.5V</td>
<td>1.8W</td>
<td>0.2V 0.1s</td>
<td>No</td>
</tr>
<tr>
<td>[80]</td>
<td>1995</td>
<td>0.35µm</td>
<td>4mm²</td>
<td>±2.5 V</td>
<td>1.6W</td>
<td>0.2V 0.1s</td>
<td>No</td>
</tr>
<tr>
<td>[90]</td>
<td>2000</td>
<td>0.35µm</td>
<td>4.8mm²</td>
<td>±3V</td>
<td>&lt;1W&lt;sup&gt;a&lt;/sup&gt;</td>
<td>0.5V 0.1ms</td>
<td>No</td>
</tr>
<tr>
<td>[91]</td>
<td>2005</td>
<td>Simulated 0.6µm</td>
<td>0.1mm²</td>
<td>5V</td>
<td>7.85 mW</td>
<td>-</td>
<td>No</td>
</tr>
<tr>
<td>[92]</td>
<td>2009</td>
<td>FPGA Xilinx</td>
<td>2cm²</td>
<td>3.3V</td>
<td>5W&lt;sup&gt;a&lt;/sup&gt;</td>
<td>-</td>
<td>No</td>
</tr>
<tr>
<td>[94]</td>
<td>2013</td>
<td>Discrete Simulated TL084</td>
<td>10cm²&lt;sup&gt;a&lt;/sup&gt;</td>
<td>±15V</td>
<td>2 W</td>
<td>1s 1v</td>
<td>No</td>
</tr>
<tr>
<td>[93]</td>
<td>2013</td>
<td>FPGA Xilinx</td>
<td>2cm²</td>
<td>±15V</td>
<td>5W&lt;sup&gt;a&lt;/sup&gt;</td>
<td>1V 1s</td>
<td>No</td>
</tr>
<tr>
<td>[87]</td>
<td>2015</td>
<td>Simulated 0.35µm</td>
<td>1.5mm²</td>
<td>1.4V</td>
<td>360mW</td>
<td>-</td>
<td>No</td>
</tr>
<tr>
<td>[95]</td>
<td>2016</td>
<td>Discrete</td>
<td>10cm²</td>
<td>15V</td>
<td>&lt;10W&lt;sup&gt;a&lt;/sup&gt;</td>
<td>0.2V 0.1s</td>
<td>No</td>
</tr>
<tr>
<td>[96]</td>
<td>2017</td>
<td>Simulated 0.35µm</td>
<td>2mm²&lt;sup&gt;b&lt;/sup&gt;</td>
<td>±1.2V</td>
<td>&lt;W&lt;sup&gt;a&lt;/sup&gt;</td>
<td>0.2V 0.1s</td>
<td>No</td>
</tr>
<tr>
<td>[97]</td>
<td>2019</td>
<td>Simulated 0.35µm</td>
<td>2mm²</td>
<td>3.3V</td>
<td>1.7mW</td>
<td>-</td>
<td>No</td>
</tr>
<tr>
<td>This work</td>
<td>2020</td>
<td>0.18µm</td>
<td>1.5mm²</td>
<td>1.8V</td>
<td>1.5mW</td>
<td>0.2 V 0.1s</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<sup>a</sup> This parameter is estimated based on the article.

<sup>b</sup> Capacitors implemented Off-chip.
Though the on-chip security system is in synchronization, there is an aggregating delay formed in the system that causes the system to go out of synchronization after a few ten cycles. The implementation of the $\beta$ and $\lambda$ modulators with amplifier and switch are the cause of this delay. The switches are developed with pass transistors that does not have delay compensating capacitor. Implementing better switches can reduce this delay and ensure a constant synchronization. To predict these errors usually Monte-Carlo simulation and PVT simulation is done.

Running Monte-Carlo in chaos theory is extremely challenging, especially in transient mode since the time steps for simulation need to be set manually. With the slight change of parameters because of process and mismatch the Lyapunov coefficients (Described in design section in 5.4) change. Though this change may not push the system out of the synchronization, the parameters needed for convergence change and the time step need to be changed for the system to see the chaotic result. Therefore Monte-Carlo for security sensor could not be performed. This problem exist in Lorenz circuits and there are methods, like including feedback circuits to monitor Lyapuanov coefficients to optimize CMOS design of chaotic oscillators to be robust to PVT variations, as explained in [97]. Another challenge is the connection of high frequency sensors, like the impedance sensor, to the security system. The Lorenz chaotic system implemented with Gilbert cells and integrators can not reach synchronization in frequencies higher than few kHz. To be able to have biosensors with potential sensing blocks with frequencies up to few hundred kHz other means of chaotic security other than Lorenz need to be implemented. Our temperature sensor is implemented in lower frequencies, therefore can be connected to the security system with no issue.

5.5 Conclusion

A return map immune chaotic stream cipher based on a Lorenz system is presented and realized. The designed system consumes a minimal amount of processing compared to the implementation of the same system with microcontrollers and digital encryption. The first version of the system is a PCB designed chaotic communication system integrated with a CMOS sensor. Here a temperature signal from the sensor is encrypted by the transmitter,
and the receiver decodes the signal in real-time. On-chip security with integrator and multiplexer as the main building blocks of this system is also implemented and tested experimentally. The experimental results show that with an on-chip Lorentz chaotic shift keying, a ciphering transmitter is developed. The same system can act as a decoding receiver by chaos synchronization. Sensors integrated with analog-based chaotic encryption show great promise. These systems can be implemented with different equations and different techniques to prevent well-known attacks.
Chapter 6

Future Work and Conclusions

6.1 Original Contribution and Discussion

In this work, a secure impedance and temperature sensor has been presented. Both sensors step further than the state-of-art design by providing low power, low-area designs with frequency output. The impedance sensor performs a 2 phase resistance and capacitance measurement using current comparison and voltage comparison respectively. This design eliminates the need for an accurate 90° out of phase signal that is challenging and area consuming to implement. The temperature sensor uses sub-threshold CMOS technology and window voltage comparators to translate the temperature to voltage. The capacitor needed for this sensor is a few pF, facilitating the implementation of this sensor on-chip.

The implementation of integrating analog security with sensors is then presented that takes the initial step towards having hardware-based integrated security encryption in any IoT and arrayed sensor systems. This on-chip multi-modal system securely transmits and receives the data. The security measure is a real-time chaotic ciphering block that will decipher the message through synchronization of a similar block. The ciphering block is implemented using low power integrators and multipliers. Both these blocks are adjustable from outside the chip using biasing currents. This is the first implementation of sensors with chaotic ciphering on the same chip. The transmitter/receiver system is also the first to eliminate attacks using time scaling parameter. The power consumption of the integrated ciphering block is a magnitude of an order lower than security implemented using discrete
parts, and 2 magnitudes of orders lower than security implemented by FPGA boards using the same method of ciphering. This decrease in power show this method as a promising method to implement security in portable, wearable devices in the age of quantum computing.

Though other developed system shows successful synchronization and is a means of being immune to attacks, there is still much room for the system’s improvement to reach a system that is ready for commercialization. Wearable devices are the new norm of this generation. The race between companies is to provide different types of accurate sensors on wearables and have the devices FDA approved. Besides temperature and impedance, various other sensors are beneficial to have on wearable sensors. pH sensors and pulse oximeters are among the most common ones.

At the start of 2020, we witnessed a pandemic overtake the world. The Covid-19 pandemic has generated increased awareness of the significant advantages and possibilities of monitoring outside of hospital environments. Current WHO guidelines emphasize on Covid-19 patient monitoring based on fever indications, respiratory distress, and blood oxygen availability. All research for the last couple of years point out only small advancements in studies involving wearable devices from companies. Companies mostly consist of startups and small businesses scattered around the world, with research areas that are far from each other. The difference in the focus of wearable devices grants the advantage of providing different views on a single problem. Different numbers of sensors integrated into a single device from different companies [53, 119, 120, 121], show the feasibility of having a single device with many sensing devices and the necessity of having a cloud data center for professionals to have real-time and accessible connection to the data. The disadvantage is the lack of a wholesome portable sensing system to monitor patients in the current influenza pandemic. In the world of commercial FDA cleared health monitoring wearable devices, which is a rapidly growing and definitely not a small world, currently, there is no wholesome wearable device capable of sensing common symptoms of influenza that has affected the respiratory system. The presented array-able sensors can be integrated with other sensors to be the first system for influenza patient monitoring.

In terms of security improvements, there have been various implementations of chaotic system published in literature. However, not many have been implemented experimentally
or used for chaotic communication. Different chaotic equations can be tested, some with just a few tens of transistors to have a system with secure communication. There are also numerous attacks with techniques to prevent them. The developed system can be improved by implementing a driving circuit to remove the various biasing needed and a control system to detect the Lyapunov parameters and ensure chaotic behavior before encoding the signal. Higher frequency chaotic communication are also among the most recent research.

6.2 Future Work

The outlook of this research ranges from implementing more and improved sensors to have a better security scheme. These further steps can be added to this trending research:

1. More sensors (for example, PH, humidity sensor, ECG) can be integrated with the existing sensors to have a complete standalone sensing system. Different applications can be defined for multi-modal sensors. An application can be a pH, temperature, and impedance sensors arrayed as the base of a smart culture dish that not only monitors the impedance of cells for disease diagnosis but also extracts real-time cell growth data from the pH, humidity, and temperature of the cellular micro-environment. Another application is patient monitoring using wearable sensors, including temperature, impedance, pulse oximeters, and pH sensor. We are living in a world overtaken by the COVID-19 pandemic. Having a wearable impedance and temperature sensor along with a pulse oximeter that is low-power and cheap can be helpful in controlling a pandemic and patients with respiratory diseases.

2. In the case of wearable devices, using nano-fabricated electrodes will be considered for the design. New noninvasive/minimally invasive nano-electrodes can be used as patches to measure physiological data from human body. The most critical problem of these electrodes is their fabrication in a different process than CMOS fabrication.

3. Another part of the project, very interesting to be developed is a wireless transmitter capable of sending chaotic signal. Using the current data processing blocks does not eliminate the need for a wired synchronization line, which is hard to implement in wireless devices. Generally, off-chip RF or Bluetooth modules are the most power-consuming blocks of any wearable/Sensor system. In the case of the impedance measurement system, the RF
transmitter used 3 mW, almost 200 times more power consumption than the impedance sensor. Having a low-power wireless sensor fabricated on-chip will eliminate the need for power-consuming data transfer blocks.

4. Various equations can be implemented with electronic circuits to provide chaos. These circuit implementations can also be different for a single equation. These implementations can enable synchronization in higher frequencies and a greater number of states for increased security. Newer methods implemented in circuits to prevent different attacks can be developed. It must be noted that any additional circuits to prevent different attacks will add to the power consumption and area.


necklace to measure stroke volume, cardiac output and thoracic impedance,” *Journal of the American College of Cardiology*, vol. 67, no. 13 Supplement, p. 1296, 2016. 10


[65] W. Yang, H. Jiang, and Z. Wang, “A 0.0014 mm2 150 nw cmos temperature sensor with nonlinearity characterization and calibration for the 60 to 40°C measurement range,” *Sensors*, vol. 19, no. 8, p. 1777, 2019. ix, 19, 20, 62


[67] K. Souri, Y. Chae, F. Thus, and K. Makinwa, “A 0.85 v 600nw all-cmos temperature sensor with an inaccuracy of 0.4 °c from - 40°C to 125°C,” *IEEE ISSCC Digital Technology Papers*, pp. 222–223, 2014. 19, 62


[71] D. Prasad, V. Nath, V. Vishwanthan, and M. Mehta, “A 0.6 v 117 nw high performance energy efficient system-on-chip (soc) cmos temperature sensor in 0.18 µm cmos for aerospace applications,” *Microsystem Technologies*, vol. 25, no. 6, pp. 2301–2311, 2019. 21, 62


Appendix
A  Layouts and testing conditions of the proposed circuits

In this appendix layouts of the design along with information about biasing the circuits is included.

A.1  Impedance sensor

The layout of the impedance sensing system implemented in 180 nm is shown in Fig. 1. The impedance sensing system use the stimulating sinusoidal signal of 0.5 V amplitude and frequency of 1 kHz applied by a function generator. The same signal is applied to the in-phase input of the voltage comparator. The other input of the voltage comparator is a 0.5 DC voltage applied by a power supply. When converting the pulse width to frequency a 2 MHz, 1.8 V peak-to-peak pulse signal is applied to the SR latch as the modulating signal from another function generator. The supply voltage for all blocks is 1.8 V.

**Figure 1:** Layout of impedance sensing system chip fabricated in 180 nm technology.
A.2 Temperature sensor

For the temperature sensor, the amplifier has a biasing pin to apply the bias current of 10 $\mu$A. The bias current is implemented with a passive resistor off chip. The supply voltage for each temperature sensor was set as low as 1 V. The layout of the circuit in a standard 130 nm and 180 nm technology is shown in Fig. 2 and Fig. 3. The charging capacitor is implemented on chip capacitor, but the scaling resistor is a 220 $\Omega$ off chip resistor. In the chamber temperature test to ensure a stable reference voltage for the window comparators, the low voltage reference of 0.6 V and 1.2 V is applied by voltage supplies. This voltage window define the speed of system since charge and discharge of capacitor happens in this window.

A.3 Security sensor

All blocks of the security ciphering where implemented using $\pm0.9$ V. The multiplexer does not need outside biasing. The biasing of the amplifier for the Beta and Lambda modulator was implemented by a potentiometer off chip, we swept the biasing current from 10 $\mu$A to
20\mu A to see the largest voltage for the output of chaotic signal. The implementation of this bock in 180 nm is shown in Fig. 4.

The integrator is implemented with 4 stage of $g_m$ and $1/g_m$ blocks, all having their own current bias implemented by a passive resistor off-chip. For the 180 nm design I1 and I3, the $g_m$ block biases are 8 nA in our design and the $1/g_m$ block biases are 27 nA. The OTA
stage driving the output capacitor has 3 biases implemented off chip using passive resistors, the biasing currents for this stage is 10 nA. For the 130 nm design I1 and I3, the $g_m$ block biases are 32 nA in our design and the $1/gm$ block biases are 27 nA. The OTA stage driving the output capacitor has 3 biases implemented off chip using passive resistors, the biasing currents for this stage is 1.7 uA. The Layout of Gilbert cell implemented in 180 nm and 130 nm-BiCMOS is shown in Fig. 5 and Fig. 6.

The Layout of Gilbert cell implemented in 130 nm-BiCMOS and 180 nm is shown in Fig. 7 and Fig. 8 respectively. The input current bias to test the Gilbert cell is 14 µA set by a potentiometer off chip. Two resistor of 70 KΩ is also implemented off chip. Though these resistors need for biasing the circuit are implemented off chip, all blocks along with the scaling resistors of Lorenz circuit fit on a 1.5 mm² chip as shown in Fig. 9.
Figure 6: Layout of integrator fabricated in 130 nm technology.
Figure 7: Layout of Gilbert Cell fabricated in 180 nm technology.
Figure 8: Layout of Gilbert Cell fabricated in 130 nm technology.
Figure 9: Layout of security system fabricated in 180 nm technology.
Vita

Ava Hedayatipour received her B.S. degree in electrical engineering from the Iran University of Science and Technology, Iran, in 2012, and the M.S. degrees in electrical engineering from Shahid Rajaee Teacher Training University, Tehran, Iran, in 2015. In 2016, she joined the Department of Electrical Engineering, University Tennessee Knoxville, as a research and teaching assistant pursuing Ph.D. degree in electrical engineering. Her current research interests include analog integrated circuit designs, bio-implantable and biomedical devices, low-power and low-noise designs, microelectronics, mixed signal VLSI designs, hardware security and semiconductor devices.