

POWER OPTIMIZED PROBABILISTIC SENSING

BY

IBRAHIM ABDULRAHMAN ALBULUSHI

A Thesis Presented to the
COLLEGE OF GRADUATE AND INTERDISCIPLINARY STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

ELECTRICAL ENGINEERING

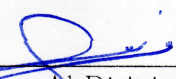
JUNE 2024

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
DHAHRAN 31261, SAUDI ARABIA

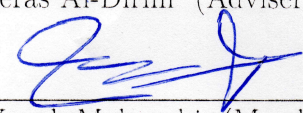
DEANSHIP OF GRADUATE STUDIES

This thesis, written by **IBRAHIM AL-BULUSHI** under the direction of his thesis adviser and approved by his thesis committee, has been presented to and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN ELECTRICAL ENGINEERING**.

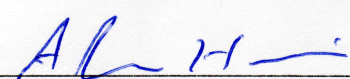
Thesis Committee


Dr. Feras Al-Dirini (Adviser)

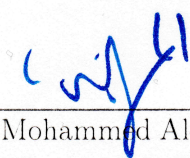
2/6/2024


Dr. Yaqub Mahnashi (Member)

June 2nd, 2024


Dr. Alaa El-Din Hussein (Member)

June 2nd, 2024


Dr. Mohammed Al-Muhaini
Department Chairman


Dr. Suliman Al-Homidan
Dean of Graduate Studies

Date



©Ibrahim Al-Bulushi
2024

This thesis is dedicated to all those who have shaped my journey and contributed to my growth, both personally and professionally. To my mother Rugayyah Al-Bulushi, my brothers Abdulrahim, Abdulkareem, Abdullah and Tariq, my sisters Sadiyyah, Sara and Aeshah, whose unwavering love and sacrifice have been the bedrock of my life. Your endless support and belief in my potential have been my greatest source of strength and motivation. This work stands as a testament to your enduring faith and encouragement.

ACKNOWLEDGMENTS

All praises are to Allah, I am very grateful to Allah for His mercy and protection for me to complete this work as well as my master's program successfully. Peace and blessing be always upon to the Prophet Muhammad, his family, his companions, and his followers until Hereafter. I am deeply humbled and grateful for the opportunity to express my heartfelt thanks to those who have supported and guided me throughout this journey. To my advisor and mentor Dr. Feras Al-Dirini, your profound wisdom, patience, and guidance have been invaluable. Your commitment to my growth, both academically and personally, has been a beacon of light throughout this journey. The countless hours you have dedicated to nurturing my ideas and challenging me to excel have shaped me in ways words cannot fully capture. Your guidance, advice, ideas, enlightenment and support have shaped the core of my research skills. I am grateful to the committee members, Dr. Yaqub Mahnashi, Dr. Alaa El-Din Hussain, for their constructive comments and suggestions that greatly enhanced the quality of this work. I am also thankful to Mr. Saleh Bunaiyan for sharing with me the important data that built my thesis, for explaining to me the methods and the ideas behind such a topic, for sharing with me the novel design that he invented, simulations and codes. I am also grateful to Dr. Furqan Zahoor for giving me the idea to include the encryption to my design and how to verify it through the NIST test suite, also sharing the NIST

test suite code with me which strengthened my work. I am grateful to my friends Hamid Al-Mehdhar, Adnan Muneer, Mohammed Al-Jizani, whose encouragement and understanding have been a source of comfort and motivation. Your belief in me and your willingness to stand by me through every challenge has been a gift beyond measure. I would like to express my deepest gratitude to my family, whose unwavering support and love have been the cornerstone of my journey. Your encouragement and belief in me have provided the strength and motivation to pursue my dreams and overcome challenges. To my mother Ruqayyah Al-Bulushi, your boundless love, sacrifice, and guidance have been the foundation upon which I have built my life. Your wisdom, patience, and belief in my potential have been a constant source of inspiration. Words cannot fully capture the depth of my appreciation for all that you have done for me. Your support has been my guiding light, and this achievement is as much yours as it is mine. I am thankful to King Fahad University of Petroleum and Minerals (KFUPM) for giving me such an opportunity to complete my master's program. To all those whose paths I have crossed, whether briefly or enduringly, your kindness and encouragement have touched my heart and spirit. Each of you has contributed to this achievement in significant ways, and I carry your support with deep gratitude.

TABLE OF CONTENTS

ACKNOWLEDGMENTS	iv
LIST OF TABLES	ix
LIST OF FIGURES	x
LIST OF SYMBOLS	xiii
LIST OF ABBREVIATIONS	xiv
ABSTRACT (ENGLISH)	xvi
ABSTRACT (ARABIC)	xviii
CHAPTER 1 INTRODUCTION	1
1.1 Motivation from the Neural System	2
1.2 Data Acquisition Approaches	3
1.3 Probabilistic Sensing	4
1.4 Security and Encryption	7
1.5 Thesis Organisation	8
CHAPTER 2 LITERATURE SURVEY	9
2.1 Analog Feature Extraction	9
2.1.1 Keyword-Spotting	10
2.1.2 Voice Activity Detection	13
2.1.3 Other Types of Event Detection	17

2.1.4	Outcome of Surveying Feature Extraction Designs	19
2.2	Probabilistic Sensing	20
2.3	In Sensor Data Encryption	22
CHAPTER 3	RESEARCH GOALS	25
3.1	Intelligence	26
3.1.1	Number of Features Captured	26
3.1.2	Probabilistic Activation Instead of Deterministic	27
3.2	Autonomy	28
3.2.1	Energy Efficiency	28
3.2.2	Real-Time Event Detection	29
3.2.3	Detection Delay	30
3.3	Security	30
3.3.1	In Sensor Data Encryption	30
CHAPTER 4	MAIN CONTRIBUTIONS	33
4.1	Analog Feature Extraction	33
4.2	Probabilistic Sensing	33
4.3	In Sensor Data Encryption	34
CHAPTER 5	SYSTEM DESIGN	35
5.1	Overall System Architecture	35
5.2	Detailed System Design	38
5.2.1	Analog Feature Extraction	38
5.2.2	Probabilistic Sensing	40
5.2.3	In Sensor Data Encryption	42
CHAPTER 6	SYSTEM IMPLEMENTATION	44
6.1	Emulating the P-bit Behaviour in FPGA Board	44
6.2	Proposed Trivium Circuit Design	47

CHAPTER 7	RESULTS	50
7.1	Experimental Setup	50
7.2	Analog Feature Extraction	53
7.3	Probabilistic Sensing	55
7.4	In Sensor Data Encryption	59
CHAPTER 8	DISCUSSION AND FUTURE WORK	64
8.1	Discussion	64
8.2	Future Work	65
CHAPTER 9	CONCLUSION	67
APPENDIX A	SUPPLEMENTARY MATERIAL	69
REFERENCES		74
VITAE		83

LIST OF TABLES

Table 2.1	Comparison of the Detection Delay Among the Examined Existing Feature Extraction Designs.	19
Table 2.2	Comparison Between the Existing Encryption Algorithms. . .	24
Table 7.1	Detection delay parameters and power consumption comparison between the original design and the proposed design. . . .	55
Table 7.2	NIST Test Suite Evaluation.	61
Table 7.3	Experiment NSME Values with Sample Saving.	63
Table 7.4	Simulation NMSE Values with Sample Saving.	63

LIST OF FIGURES

Figure 1.1	A diagram depicting the spinal reflex arc's response within the ANS to external stimuli [3].	2
Figure 1.2	Overall system design for autonomous data acquisition [3]. . .	3
Figure 1.3	Comparison of event-based data acquisition methods. (a) demonstrating the simple feature extraction followed by encoding stage to receive the data as spikes train. (b) activation-based data acquisition unit consisting of feature extraction and activation unit [3].	4
Figure 1.4	A proposed system architecture for probabilistic autonomous data acquisition, showcasing the utilization of a p-bit as a probabilistic activation unit for data collection and an op-amp utilized as a deterministic activation unit.	5
Figure 2.1	AFE design of [16].	11
Figure 2.2	AFE design of [17].	12
Figure 2.3	AFE design of [18].	12
Figure 2.4	AFE design of [19].	13
Figure 2.5	AFE design of [20].	14
Figure 2.6	AFE design of [21].	14
Figure 2.7	AFE design of [22].	15
Figure 2.8	AFE design of [23].	15
Figure 2.9	AFE design of [24].	16
Figure 2.10	AFE design of [25].	16
Figure 2.11	AFE design of [26].	17

Figure 2.12	AFE design of [27].	18
Figure 2.13	AFE design of [29].	18
Figure 5.1	Block diagram demonstrating the over all system architecture including all the units (e.g., AFE unit, Activation unit, Data acquisition unit and Encryption unit.	36
Figure 5.2	Proposed component-level circuit design.	37
Figure 5.3	Magnet fluctuation dynamics for various types of magnets are analyzed. The simulations provide sample probability distributions of magnetization for: (a) a circular In-Plane Magnet Anisotropy (IMA), (b) an isotropic magnet, (c) a Low Barrier Magnet (LBM) with IMA, and (d) a LBM with Perpendicular Magnetic Anisotropy (PMA). [3].	40
Figure 5.4	Proposed design Trivium stream cipher block diagram demonstrating the mechanism of how the key stream is developed and the operation to cipher the plain text message and deciphering it.	42
Figure 6.1	Proposed FPGA based p-bit design, showcasing the main blocks of the design, the output of the comparator is ANDed with a clock of 2000 samples per second.	45
Figure 6.2	Proposed FPGA based p-bit design with the AFE unit taking its input directly to the activation function of the.	46
Figure 6.3	Component level implementation of the proposed modified Trivium stream cipher circuit design.	47
Figure 7.1	Experimental setup illustrating the AFE circuit with all of the stages and the interconnection between the IC's and the passive components.	51
Figure 7.2	Experimental setup illustrating the AFE circuit and the MYRIO-1900 with the connections of the analog inputs and outputs as well as the digital inputs and outputs.	52

Figure 7.3	For a sine wave input to the AED, the blue curve depicts the nonideal behavior as determined by simulation. The red circles indicate regions where nonideal behavior is observed "Modified from [3]".	53
Figure 7.4	The percentage of generated samples by the probabilistic activation unit for different input voltages (V_{IN}).	55
Figure 7.5	The average random sampling rate generated by the probabilistic activation unit vs slope. The projections at the bottom of the figure display transient output samples from the probabilistic activation unit for various data points on the curve corresponding to different slope values.	57
Figure 7.6	Average random generated samples vs slope demonstrated for the proposed modes of operation.	58
Figure 7.7	The behaviour of the sampling based on the mode of operation. Each mode was achieved by varying the value of V_{ref} in simulation, and varying the LFSR range in experiment. . . .	59
Figure A.1	Results for the probabilistic autonomous data acquisition and in sensor encryption part 1, events 1 - 7.	70
Figure A.2	Results for the probabilistic autonomous data acquisition and in sensor encryption part 2, events 8 - 14.	71
Figure A.3	Results for the 50 events used to calculate the NMSE part 1, events 1 - 24	72
Figure A.4	Results for the 50 events used to calculate the NMSE part 2, events 25 - 48	73

LIST OF SYMBOLS

$\| \cdot \|$ The Norm of a Vector

LIST OF ABBREVIATIONS

ADC	Analog to Digital Converter
AED	Analog Event Detection
AES	Advanced Encryption Standard
ANS	Autonomous Nervous System
BNN	Binarized Neural Network
BPF	Bandpass Filter
CLT	Curve Length Transform
CNN	Convolutional Neural Network
DES	Data Encryption Standers
ECG	Electrocardiography
FETs	Field-Effect Transistors
FPGA	Field-Programmable Gate Array
GSCD	Google Speech Command Dataset
ILO	Injection-Locked Oscillator
IMA	In-Plane Magnet Anisotropy
IV	Initialization Vector

LBM	Low Barrier Magnet
LFSR	Linear Feedback Shift Register
MFCC	Mel Frequency Cepstral Coefficients
NLFSRs	Non-Linear Feedback Shift Registers
NMSE	Normalized Mean Squared Error
p-bit	Probabilistic Bit
PMA	Perpendicular Magnetic Anisotropy
QNRC	Quantum Noise Random Stream Cipher
RNGs	Random Number Generators
SAC	Sparsity-Aware Computation
sMTJ	stochastic Magnetic Tunnel Junction
SNR	Signal to Noise Ratio
SoC	System-On-Chip
SotA	State-of-the-Art
SQ	Sparsified Quantization
TD-CNN	Time-Domain Convolutional Neural Network
TRNG	True Random Number Generator

THESIS ABSTRACT

NAME: IBRAHIM ABDULRAHMAN AL-BULUSHI
TITLE OF STUDY: POWER OPTIMIZED PROBABILISTIC SENSING
MAJOR FIELD: ELECTRICAL ENGINEERING
DATE OF DEGREE: JUNE 2024

In many situations, data tends to be sparse, containing extensive redundant information. Nonetheless, current data acquisition systems often ignore this redundancy, continuously collecting and processing data without considering its actual value. Lately, there has been a growing focus on autonomous systems that respond specifically to meaningful information or events. This shift is crucial for Internet-of-Things (IoT) devices, to prevent the unnecessary processing and communication of any redundant information, which in turn will save the overall power of the system. In this thesis, several novel contributions and optimizations to the concept of autonomous data acquisition are presented, specifically focusing on the experimental implementation of probabilistic autonomous data acquisition (termed here as probabilistic sensing) using a Probabilistic Bit (p-bit). For the first time, probabilistic sensing is experimentally demonstrated using a p-bit in an experimental setup employing a Field-Programmable

Gate Array (FPGA) implementation of the p-bit, and achieving results comparable to those obtained with stochastic Magnetic Tunnel Junction (sMTJ) in simulations. Additionally, the concept of stochastic unit sharing amongst different p-bits driving different applications is experimentally demonstrated. The two different applications implemented are probabilistic sensing and in-sensor data encryption. The stochasticity of the p-bit is utilized to provide a random input sequence to the encryption unit. A novel modified Trivium ciphering technique has been implemented using the FPGA board, utilizing much fewer logic gates and a single shift register, making it suitable for power-constrained applications. Furthermore, to enhance the autonomy of the data acquisition approach an additional event feature detection mechanism is incorporated into the design of the Analog Feature Extraction (AFE) circuit, while still reducing the power consumption of the AFE unit by 70% through the use of clippers. The designed system was tested on seismic data obtained from an active seismic survey. The use of probabilistic autonomous data acquisition instead of deterministic autonomous data acquisition has resulted in an overall power saving improvement of the system from 69% to 93% during the occurrence of active seismic events, while still preserving the system's rapid real-time response required for autonomous data acquisition.

ملخص الرسالة

الاسم:

إبراهيم عبدالرحمن البلوشي

عنوان الدراسة:

إستشعار إحتمالي منتظم الطاقة

التخصص:

قسم الهندسة الكهربائية

تاريخ الدرجة العلمية: ذو القعدة 1445

في العديد من الحالات، تميل البيانات إلى أن تكون متناثرة، تحتوي على معلومات زائدة عن الحاجة بشكل واسع. ومع ذلك، فإن أنظمة جمع البيانات الحالية غالبًا ما تتجاهل هذه المعلومات الزائدة، حيث تقوم بجمع ومعالجة البيانات بشكل مستمر دون النظر في قيمتها الفعلية. في الآونة الأخيرة، كان هناك تركيز متزايد على الأنظمة المستقلة التي تستجيب تحديدًا للمعلومات أو الأحداث المهمة. هذا التحول مهم لأجهزة إنترنت الأشياء، لمنع المعالجة والاتصال غير الضروريين لأي معلومات زائدة، مما سيؤدي بدوره إلى توفير الطاقة الكلية للنظام. في هذه الأطروحة، يتم تقديم عدة مساهمات وتحسينات جديدة لمفهوم جمع البيانات المستقل، مع التركيز بشكل خاص على تجربة جمع البيانات المستقل الاحتمالي (الذي يطلق عليه هنا الاستشعار الاحتمالي) باستخدام البت الاحتمالي. لأول مرة، يتم إثبات الاستشعار الاحتمالي تجريبيًا باستخدام البت الاحتمالي في إعداد تجريبي يوظف تنفيذ مصفوفة البوابات المنطقية القابلة للبرمجة للبت الاحتمالي، وتحقيق نتائج قابلة للمقارنة مع تلك التي تم الحصول عليها باستخدام الوصلة النفقية المغناطيسية العشوائية في المحاكاة. بالإضافة إلى ذلك،

يتم إثبات تجريبيًا مفهوم مشاركة الوحدات العشوائية بين مختلف البت الاحتمالي التي تدير تطبيقات مختلفة. التطبيقات المختلفة التي تم تنفيذها هي الاستشعار الاحتمالي وتشفير البيانات داخل المستشعر. يتم استخدام العشوائية في البت الاحتمالي لتوفير تسلسل إدخال عشوائي لوحدة التشفير. تم تنفيذ تقنية تشفير (تريفيوم) المعدلة الجديدة باستخدام لوحة مصفوفة البوابات المنطقية القابلة للبرمج، باستخدام عدد أقل بكثير من البوابات المنطقية ومسجل تبديل واحد، مما يجعلها مناسبة للتطبيقات التي تقيّد الطاقة. علاوة على ذلك، لتعزيز الاستقلالية في نهج جمع البيانات، تم دمج آلية اكتشاف ميزات الأحداث الإضافية في تصميم دائرة استخراج الميزات التناظرية، مع تقليل استهلاك الطاقة لوحدة دائرة استخراج الميزات التناظرية بنسبة 70% من خلال استخدام القاطع. تم اختبار النظام المصمم على بيانات زلزالية تم الحصول عليها من مسح زلزالي نشط. استخدام جمع البيانات المستقل الاحتمالي بدلاً من جمع البيانات المستقل الحتمي أسفر عن تحسين توفير الطاقة الكلي للنظام من 69% إلى 93% خلال حدوث الأحداث الزلزالية النشطة، مع الحفاظ على استجابة النظام السريعة في الوقت الحقيقي المطلوبة لجمع البيانات المستقل.

CHAPTER 1

INTRODUCTION

IoT system bottlenecks arise from sensors continuously collecting enormous volumes of data due to the rapid growth of technology and their hunger for more data to deliver the best possible output. Processing, analyzing, and storing large amounts of data becomes difficult due to their massive magnitude. IoT includes a broad range of devices, from professional industrial instruments to everyday domestic items. By 2025, it is anticipated that the number of IoT-connected devices worldwide will reach around 20 billion, an increase from the current estimate of 18 billion. This bottleneck has created a need for sensors that can collect and interpret data locally with the aim of determining which data is necessary for sensors to connect with other IoT devices on their own. By this strategy network-level congestion may be relieved [1]. Present approaches frequently return the processing burden to energy-constrained sensor nodes. The goal is to move the emphasis from processing data to secure and reliable intelligent data collection that will minimize energy waste from processing unnecessary data by giving sensors the ability to decide what information to capture and what to discard [2].

1.1 Motivation from the Neural System

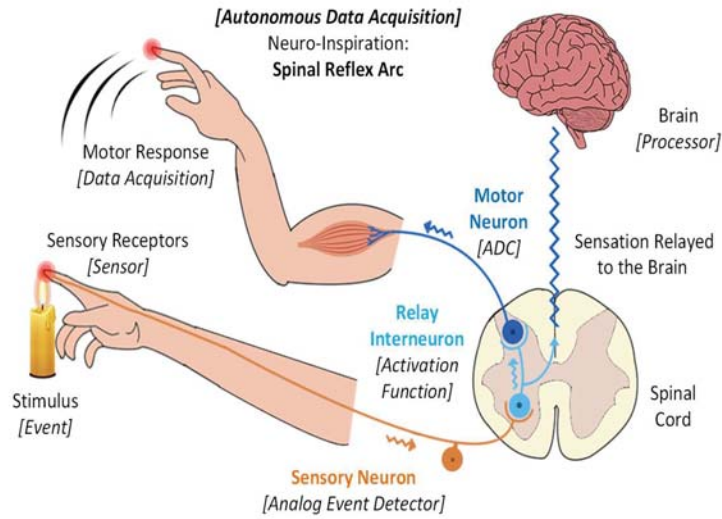


Figure 1.1: A diagram depicting the spinal reflex arc's response within the ANS to external stimuli [3].

The core of this thesis is to introduce the idea of an Analog Event Detection (AED) technique. It is intended for this method to quickly decode analog sensor outputs and produce digital control signals. This would enable system blocks to be selectively activated only in response to pertinent stimuli, saving power during non-event times. The motivation draws inspiration from the efficiency of the Autonomous Nervous System (ANS) found in biological systems as illustrated in Figure 1.1 [3]. The ANS processes sensory stimuli locally and autonomously triggers responses without involving the brain in every decision. The goal is to mimic this efficiency in sensor data acquisition.

1.2 Data Acquisition Approaches

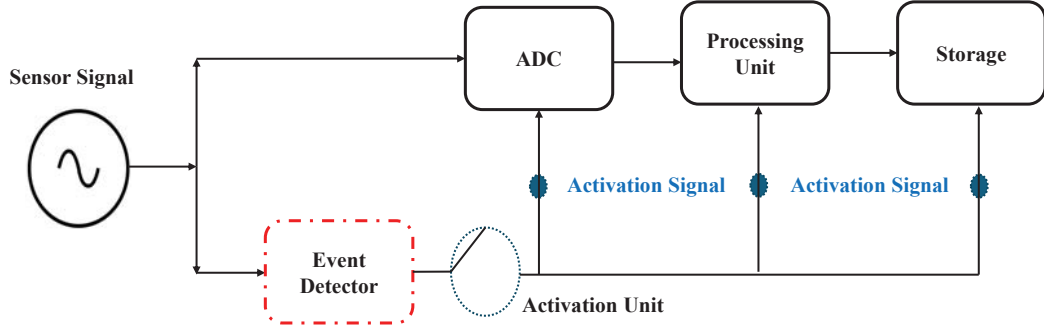


Figure 1.2: Overall system design for autonomous data acquisition [3].

The idea behind the event driven data acquisition scheme is shown in Figure 1.2, where the signal of the sensor would access the AED circuit in analog form, it will be processed very fast in the analog domain. Consequently, it would produce a digital control signal which will be responsible for activating the remaining system blocks. Furthermore, Figure 1.3(a) shows the approaches used for data acquisition and they are mainly two approaches used. The first approach focuses on encoding specific signal characteristics, such as amplitude fluctuations or frequency variations, into discrete values or spike trains. Thus, moving away from the conversion of the actual amplitude, which in turn consumes a considerable amount of power. Noncontinuous “event-based” sampling techniques are utilized in various applications since plenty of features of the signals are stable and do not change continuously. Hence, it leads to the generation of asynchronous non-uniformly sampled data points. These approaches hold promise and significance in certain applications where the signal features contain essential information, as demonstrated in event-based cameras, for instance, [4], [5]. As a result, reconstructing the original signal might prove unfeasible or require extensive

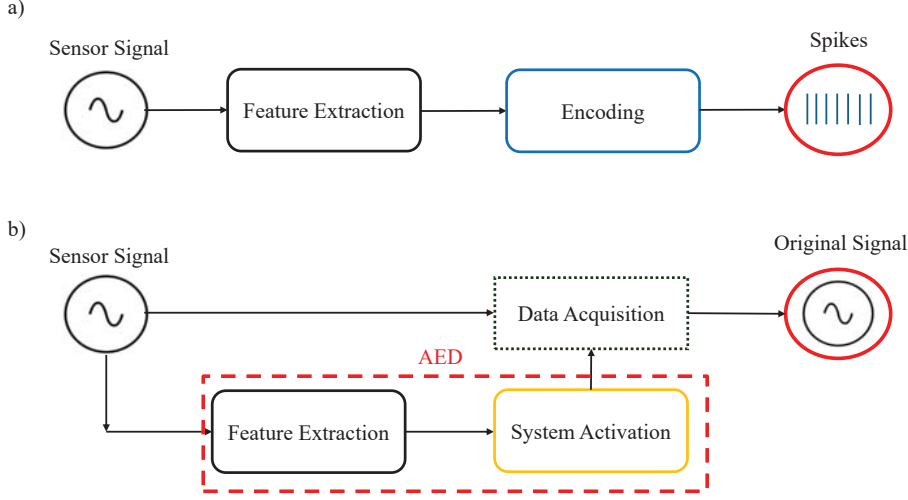


Figure 1.3: Comparison of event-based data acquisition methods. (a) demonstrating the simple feature extraction followed by encoding stage to receive the data as spikes train. (b) activation-based data acquisition unit consisting of feature extraction and activation unit [3].

post-processing, which may be incompatible with today’s digital systems. The second approach in Figure 1.3(b) shows that the data path is dispatched from the control path in the autonomous data acquisition scheme [6][7], enabling the processing of samples in the event-based control while retaining the ability to capture the original input signal waveform at a high resolution.

1.3 Probabilistic Sensing

Lately, various approaches have been developed that prioritize selectivity over flexibility in data acquisition through event-based sensing. These methods selectively capture specific aspects of the signal associated with an event—typically detected in real-time within the analog domain—or sometimes the entire signal itself, but only when specific

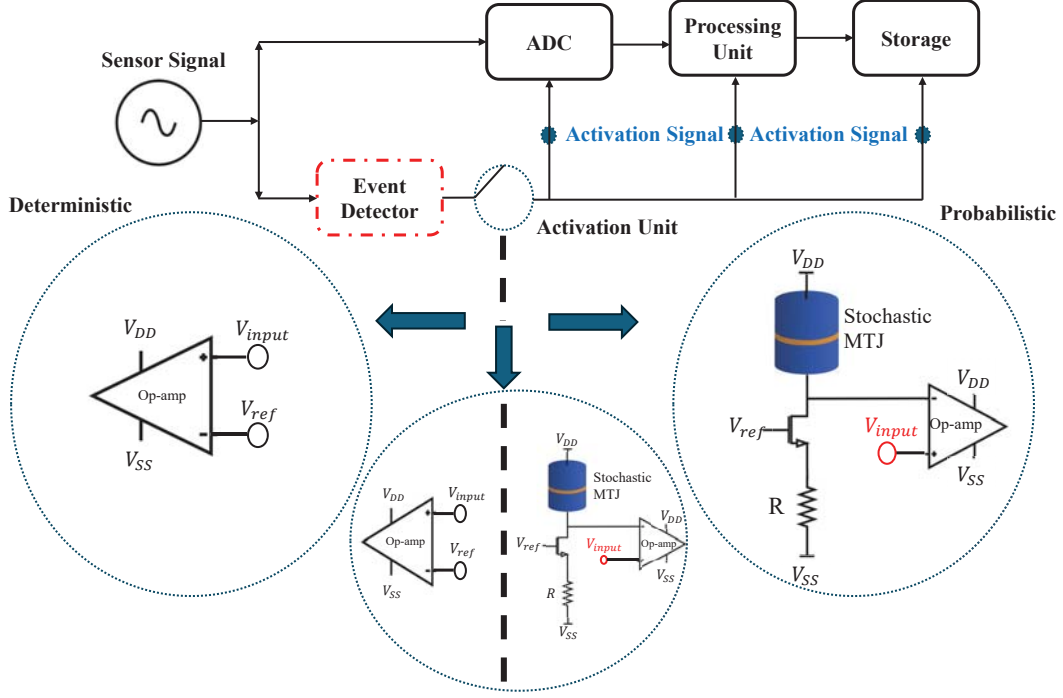


Figure 1.4: A proposed system architecture for probabilistic autonomous data acquisition, showcasing the utilization of a p-bit as a probabilistic activation unit for data collection and an op-amp utilized as a deterministic activation unit.

events occur [8]. Selective data acquisition methods can lead to a significant improvement in sensitivity, which is crucial for detecting low abundance signals. By focusing on specific features of an event signal, selectivity can enhance the accuracy of the data collected. Additionally, selectivity allows for the efficient use of computational and storage resources by only capturing data that is relevant to the event of interest. The ability to identify events of interest in real-time within the analog domain allows for immediate processing and decision-making [9]. Such an approach involves a crucial, irreversible decision: whether or not to sample. Nevertheless, integrating this extra probabilistic data with the actual sensor readings presents a complex challenge when using deterministic digital encoding techniques. Although this decision may seem straightforward, it is often challenging to distinguish between the onset of a genuine

event and a false one, necessitating a degree of probabilistic judgment. The developing field of probabilistic computing presents a sophisticated method for integrating probabilistic data within the time-based fluctuations of a bit, known as a probabilistic bit or p-bit [10]. A p-bit functions like a traditional digital bit by representing information as ‘1’ or ‘0’. Yet, unlike a fixed digital bit, a p-bit oscillates between these states in a controlled, random fashion. This unique behavior enables it to naturally incorporate probabilistic data within its time-based variations. The probabilistic event-detection unit mimics the function of a sensory neuron by initiating the operation of the entire system, including the data acquisition component the Analog to Digital Converter (ADC) rather than producing a fixed outcome, the employment of a p-bit allows for a response that is based on probability. This process is achieved by capturing the analog characteristics of events from the sensor’s signal as they occur and feeding these characteristics into a p-bit. The p-bit, in turn, acts as a trigger mechanism, as illustrated in Figure 1.4. This approach allows for an independent and event-driven method of collecting data from sensors that have limited energy. It does this by incorporating a level of probabilistic certainty into the timing of the data collection process. The p-bit triggers the data collection process when it clearly identifies an event. If it doesn’t detect any event, it ensures that the rest of the system, including the data acquisition unit, remains in a low-power sleep state.

1.4 Security and Encryption

Numerous methods are commonly employed to alter data for the purpose of encryption or hiding its existence. Cryptography is one such method, ensuring the security of information in communications by means of encryption. In asymmetric encryption, a public key is used to encrypt data, while a private key, known only to the recipient, is used for decryption. On the other hand, symmetric encryption utilizes a single key for both encrypting and decrypting data. Examples of symmetric encryption algorithms include Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, among others [11]. As IoT continues to advance, an increasing volume of data needs secure exchange across openly accessible communication channels, such as wireless transmissions. Traditional encryption techniques often struggle to align with the strict limitations on resource utilization and power consumption. Trivium [12] is a streamlined stream cipher designed for hardware implementation. It was one of the top three contenders in the ECRYPT Stream Cipher Project, also known as the eStream competition, which sought to identify the most effective and concise stream ciphers [13]. The challenges of implementing effective encryption in IoT devices are multifaceted. Developers must balance the need for strong security with the constraints of limited processing power and energy resources. Furthermore, as IoT devices often communicate over wireless networks, they are particularly vulnerable to attacks such as eavesdropping, man-in-the-middle attacks, and replay attacks. Therefore, cryptographic solutions, like Trivium and others, are vital for maintaining security without overwhelming the limited capabilities of IoT hardware [14].

1.5 Thesis Organisation

The thesis is structured as follows; Chapter 2 discusses the various designs of feature extraction, p-bit, and ciphering techniques in the literature in comparison to the design proposed in this thesis. Chapter 3 presents the research goals. Moreover, Chapter 4 explains the main contribution of this thesis. Chapter 5 illustrates the overall system architecture used to implement the proposed design. System implementation and the results are described in Chapter 6 and 7 respectively. Chapter 8 discusses this thesis and potential future work to enhance the overall design. Finally, Chapter 9 concludes this thesis.

CHAPTER 2

LITERATURE SURVEY

As highlighted in the introduction, the work in this thesis aims at realizing a reliable autonomous data-acquisition system that is also secure. To achieve this, three main research domains need to be addressed: (1) Analog Feature Extraction, (2) Probabilistic Activation of Data-Acquisition (Probabilistic Sensing), and (3) In-Sensor Data Encryption. The literature on these three research domains is surveyed and summarized in the following three Sections, namely 2.1, 2.2 and 2.3, respectively.

2.1 Analog Feature Extraction

Early event detection methods, such as Post-Acquisition Digital Event Detection, initially focused on identifying events after the data had been acquired and converted into a digital format. The acquired digital data underwent processing in the digital domain to identify specific events of interest. However, this method captured all data, irrespective of relevance, leading to the transmission of both relevant and irrelevant data to other network parts. Early generations focused on reducing the communication

of irrelevant data, especially in wireless sensor network applications where minimizing communication was crucial due to power consumption in communication hardware. As AI and advanced processing became more prevalent in sensing systems, digital event detection evolved to control subsequent processing and analysis blocks. This led to better control over power usage and enhanced energy efficiency in sensing systems. Nonetheless, such approaches still suffered from the large energy budget consumed through continuous data-acquisition, regardless of how informative this data is.

To address the aforementioned problem, processing circuits custom designed to process and detect events in the Analog domain, prior to data-acquisition, have been recently pursued, with the application of keyword spotting (KWS) generally gaining a lot of attention, and the latter can also be considered as a more specific form of Voice Activity Detection (VAD), which has also attracted much attention and numerous research efforts in its own right.

Some of the most important designs presented in the literature that address these two important applications, namely KWS and VAD, are summarized in the following two subsections (2.1.1 and 2.1.2) respectively. This is followed by a summary of other types and applications of event detection in general in sub-section 2.1.3, and a summary of the overall findings of the review of the literature on this domain in sub-section 2.1.4.

2.1.1 Keyword-Spotting

The paper in [15] presents a Mel Frequency Cepstral Coefficients (MFCC) algorithm for KWS systems. Achieving an 82% reduction in multiplications and a 66% reduction

in additions, the algorithm achieves a 96.09% accuracy for ten keywords using the Google Speech Command Dataset (GSCD). The desgin was implemented in the CMOS $65nm$ technology, the circuit consumes $2.81\text{ }\mu W$ at a 1.0 V supply voltage and a 16 kHz clock, showcasing a significant 4.5x power reduction compared to similar works under the same process technology.

In [16], the paper introduces a smart and energy-efficient KWS system tailored for human-device interfaces. It suggests a switched-capacitor-based feature extractor. The implemented analog feature extractor, fabricated using a $55nm$ CMOS process, showcases notable performance. It operates with a low power consumption of $4.4\text{ }\mu W$, utilizing a 1.2 V power supply, and occupies an area of 0.39 mm^2 . During testing with the GSCD, featuring five distinct classes, the system achieves an impressive accuracy of 92.2%. The AFE design shown in Figure 2.1.

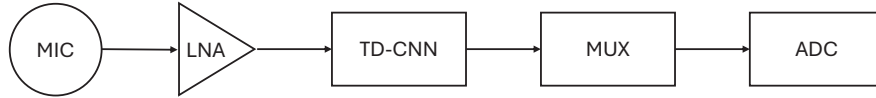


Figure 2.1: AFE design of [16].

In [17] an ultra-low power KWS system utilizing a feature extractor designed from a bandpass filter with max operator by using switched capacitor technique with Time-Domain Convolutional Neural Network (TD-CNN) for classification is proposed. In the classifier only the first layer needs an accurate calculation while the rest of the layers can binarized. The proposed design discards the use of high-precision ADC to attain a very low power KWS design. The feature extractor was fabricated using $65nm$ CMOS technology. The design consumes 270 nW to detect two keywords based

on the simulation and measurement. The AFE circuit elements is demonstrated in Figure 2.2.



Figure 2.2: AFE design of [17].

In reference [18], the article introduces a system for spotting keywords that highly prioritizes both low power consumption and high accuracy. This system utilizes analog passive switched-capacitor bandpass filters to extract MFCC features through all-analog circuits. Moreover, The analog MFCC extraction process includes various components such as the low-noise amplifier, Bandpass Filter (BPF), squarer, integrator, and discrete cosine transformer. To achieve ultra-low power and a high dynamic range, the design implements a high-order, fully differential BPF. The design is fabricated using $0.18\ \mu\text{m}$ CMOS, and the filter bank, consisting of eight BPFs, consumes only $83.2\ \text{nW}$. The overall power consumption of the feature extractor is $661.7\ \text{nW}$, resulting in a 96.6% accuracy in a two-KWS scenario. This accuracy is achieved using an FPGA based fully connected neural network with a latency of $9.6\ \mu\text{s}$. The AFE circuit is illustrated in Figure 2.3.

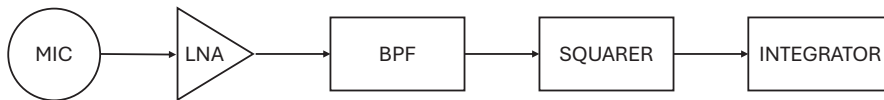


Figure 2.3: AFE design of [18].

Paper [19] proposes 2 time-mode Analog Signal Processing (ASP) circuit designs

in an analog audio feature extractor chip to solve the challenge of power and area limitations in on-device KWS. The first technique includes time-mode analog filter bank interpolation, utilizing digital XOR gates to increase the outputs of an analog bandpass filter bank. The second technique, time-mode analog rectification, makes use of a single digital XOR gate as an analog full-wave rectifier. This chip, fabricated in 65 nm CMOS technology, consumes only 80 nW and occupies 0.53 mm^2 of area while extracting a 31-element digital auditory feature vector from an input analog audio signal. The AFE archetecure is shown in Figure 2.4.

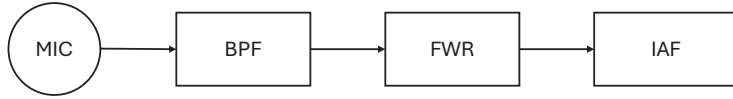


Figure 2.4: AFE design of [19].

2.1.2 Voice Activity Detection

The research detailed in [20] presents a customized acoustic frontend designed for VAD with a power consumption of under 6 W , implemented using 90 nm CMOS technology. The power-proportional sensing allows for adaptive scaling of power usage depending on the complexity of ongoing information extraction. In comparison to existing State-of-the-Art (SotA) systems, the proposed VAD system achieves a significant 10 $\times$ reduction in power consumption while maintaining an 89% average hit rate for a 12 dB Signal to Noise Ratio (SNR) in a babble context. The AFE design is shown in Figure 2.5.

The method described in reference [21] demonstrates a passive analog feature ex-

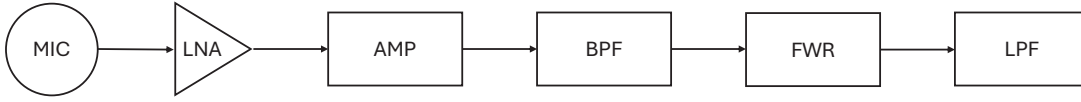


Figure 2.5: AFE design of [20].

tractor designed for VAD that prioritizes efficiency in both area and power consumption. This approach employs a switched-capacitor circuit, functioning as a TDCNN, to capture 1-bit features for the Binarized Neural Network (BNN) classifier. The model size was decreased, and the output swing was increased by taking advantage of the applied Sparsity-Aware Computation (SAC) and Sparsified Quantization (SQ) without degrading the classification accuracy. In practical testing, the VAD achieves impressive performance in speech detection with minimal power consumption 108 nW and a small area 0.8 mm^2 in a 28 nm CMOS implementation. Figure 2.6 demonstrates the AFE circuit elements.

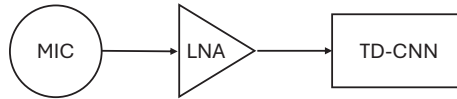


Figure 2.6: AFE design of [21].

Paper [22] presents a novel VAD that implements feature extraction in analog form and uses a neural network classification. The acoustic feature extractor contains a 12 channel Mel-filter bank that accumulates the power of different frequency bands in each time frame of the audio signal. After that the classifier uses these powers of the frequency bands as input features to decide whether it detects speech or non-speech. A Convolutional Neural Network (CNN) was used in the first-order delta-

sigma modulator. Hence, decreasing the working load for the digital domain. All the circuits were designed using 65 *nm* CMOS technology, and for the digital circuit were only Verilog-A functional modules. Figure 2.7 illustrated the AFE design.



Figure 2.7: AFE design of [22].

The study outlined in [23] presents a neural network-based acoustic sensing system with an extraordinary low power consumption of 142 *nW*. This system can perform VAD as well as identifying non-voice events. To achieve this, they implement a time-interleaved mixer-based design that sequentially scans and down-converts the 4 *kHz* bandwidth signal to a passband of less than or equal to 500 *Hz*, therefore reducing power usage in amplifiers by a factor of four. The architecture of the proposed design consists of two signal chains: an ultra-low power chain working continuously at 142 *nW* and a high performance chain consuming 18 *uW*, which activates upon event detection by the ultra low power chain. The high performance chain includes a full 4 *kHz* bandwidth analog frontend and shares the same digital backend with the ultra low power chain. The AFE design is demonstrated in Figure 2.8.

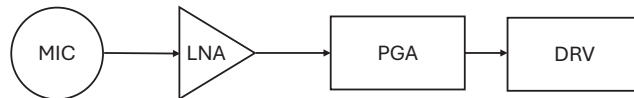


Figure 2.8: AFE design of [23].

Paper [24] introduces a VAD circuit that relies on SNR in an all-analog setup.

It achieves 99.5% accuracy in recognizing voice in household settings, while using just 760 nW from a 1.2 V power supply. The circuit optimizes energy use through an efficient analog design, utilizing continuous-time non-linear operation and fully-passive switched-capacitor processing to minimize power consumption and chip size. This VAD prototype was built using 180 nm CMOS technology. Figure 2.9 shows the AFE architecture of the proposed design.

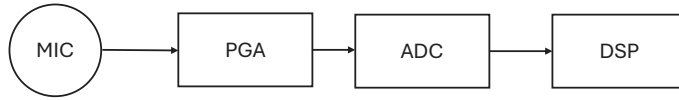


Figure 2.9: AFE design of [24].

Paper [25] discuss a design of an all-analog VAD based on neural network principles. The design employs a neural engine with weights restricted to -1, 0, and 1 value, delivering both high accuracy and minimal delay. Created using a 130 nm CMOS process, the VAD uses 28.5 μW from a 1.8 V supply and operates with a latency of just 10 ms . The accuracy rates for detecting speech versus non-speech were 94.3% and 94.1%, respectively. The AFE design is shown in Figure 2.10.



Figure 2.10: AFE design of [25].

The paper referenced as [26] introduces a highly efficient acoustic feature extractor designed for continuous VAD, mainly using ultra-low power consumption. This feature extractor utilizes a 10-channel passive switched-capacitor filter bank along-

side a passive SC envelope-to-digital converter. Through experimental validation on a prototype manufactured using a $0.18\text{ }\mu\text{m}$ CMOS process, the system demonstrates impressive performance. It achieves an average 90% speech hit rate and 86% non-speech hit rate at a 10 dB signal-to-noise ratio across all tested chips, all while maintaining a low power consumption of 270 nW . Figure 2.11 illustrates the AFE architecture of the proposed design.

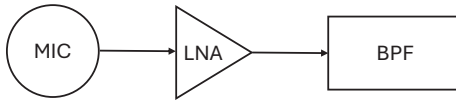


Figure 2.11: AFE design of [26].

2.1.3 Other Types of Event Detection

The document in [27] introduces an innovative filter architecture based on Injection-Locked Oscillator (ILO) designed to reduce power usage in event-driven wake-up sensing methods for IoT applications. This new architecture is integrated into a time-based filter bank for the purpose of feature extraction. In a 65 nm CMOS technological node, a four-channel ILO filter bank is implemented, showcasing a low power consumption of 6 nW specifically for the bandpass filtering function. The active area is measured at 0.0013 mm^2 , and the output dynamic range reaches 46 dB . The average power consumption per channel of the filter bank is 3 nW , covering a comprehensive bandwidth ranging from 130 Hz to 5.5 kHz . The AFE design is demonstrated in Figure 2.12.



Figure 2.12: AFE design of [27].

Paper [28] discusses a System-On-Chip (SoC) designed for speech recognition tasks like KWS and speaker verification. This chip operates with ultra low power consumption, allowing constant activation of speech-triggered interfaces in devices. It achieves this by integrating with an analog microphone, performing recognition tasks directly on the chip. In a 65 nm implementation, it achieves a worst-case power consumption of $18.3\mu W$, or $10.6\text{ }\mu W$ in typical scenarios.

In [29], there's an exceptionally low-power engine designed specifically for extracting features from Electrocardiography (ECG) signals. These signals essentially capture the heart's rhythm and contain essential components such as the QRS complex, P-wave, and T-wave, providing crucial diagnostic information about cardiovascular conditions. The feature extraction method combines the Curve Length Transform (CLT) and discrete wavelet transform and introduces a new pipelined architecture for CLT implementation. Constructed using GF 65 nm technology, the system operates at a frequency of 7.5 kHz from a 0.6 V supply voltage, consuming only 642 nW . Figure 2.13 shows the proposed design of the AFE unit.

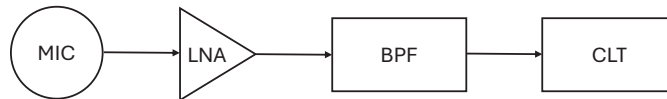


Figure 2.13: AFE design of [29].

2.1.4 Outcome of Surveying Feature Extraction Designs

Overall, the literature reviewed showcased significant reductions in power consumption of the feature extraction circuit through the utilization of advanced technologies such as 0.18- μm CMOS, 0.13- μm CMOS and 28 nm CMOS technologies. However, most of the literature overlooked the delays involved in extracting the features, which limit the application of such circuits to feature extraction and then feature acquisition, but do not allow autonomous real-time activation of data-acquisition of the original sensor signal. These delays are crucial factors in this study, as ensuring a rapid response with minimal delay is essential for enabling the achievement of real-time autonomous data acquisition. Furthermore, ?? illustrates the detection delay of the examined existing feature extraction designs.

Table 2.1: Comparison of the Detection Delay Among the Examined Existing Feature Extraction Designs.

Reference	Technology	Power consumption	Supply	Type	Detection Delay
[15]	65nm	2.81 μW	1 V	KWS	32 ms
[16]	55nm	4.4 μW	1.2 V	KWS	5 ms
[17]	65nm	270 nW	1 V	KWS	10 ms
[18]	180nm	661.7 nW	0.8 V	KWS	9.6 μs
[19]	65nm	80 nW	0.6 V	KWS	10 ms
[20]	90nm	6 μW	1.2 V	VAD	10 – 16 ms
[21]	28nm	108 nW	0.9 V	VAD	512 ms
[22]	65nm	-	0.5 V	VAD	25 ms
[23]	180nm	142 nW	-	VAD	16 ms
[24]	180nm	760 nW	1.2 V	VAD	8 – 31 ms
[25]	130nm	28.5 μW	1.8 V	VAD	10 ms
[26]	180nm	65 nW	0.65 V	VAD	50 ms
[27]	90nm	6 nW	0.4 V	Event-Based	-
[28]	65nm	18.3 μW	0.8 V	KWS-Speech	16 – 32 ms
[29]	65nm	642 nW	0.6 V	ECG	-
[6]	Discrete	65 mW	5 V	Event-Based	4.8 μs

2.2 Probabilistic Sensing

Probabilistic bits, or p-bits, are essentially adjustable Random Number Generators (RNGs). It's their distinct blend of randomness and adjustability that makes them crucial for innovative applications, especially in the realm of probabilistic computing. This ability to fine-tune them is what distinguishes p-bits from standard RNGs [30].

In paper [31], it's been demonstrated that a p-bit driven by voltage can be easily created by integrating current RNGs into a transistor circuit with the use of 2-terminal MTJs that have been proven in experiments, all without the need for inventing a new device. By applying well-known SPICE models, they illustrated that this designed p-bit can be connected to form correlated p-circuits that carry out valuable functions, such as an invertible AND gate that decomposes the output of an AND gate back into its original input pairings.

Reference [32] examines if the inherent geometric differences between devices could significantly affect a key aspect of probabilistic computing: the capacity to control probability using an external factor, like a spin-polarized current introduced into a Low Barrier Magnet (LBM). Their research suggests that this control over probability is preserved, even with the expected variations between devices. The slight discrepancies in how probability changes with current, which are normal due to device diversity, can be further reduced by enhancing the spin polarization of the current. This confirms that probabilistic computing using LBMs is resilient to minor geometric discrepancies, making it a viable option for scaling up to numerous p-bits.

Paper [33] introduces various new p-bit configurations that provide a wider scope

for adjusting input voltage and a smoother response curve. These configurations utilize both bipolar and continuous sMTJs, showcasing an enhanced ability to fine-tune over a range greater than 4 volts, which is almost half the total range of the supply voltage.

It is demonstrated in [34] that they merged sMTJ with 2D-MoS2 Field-Effect Transistors (FETs) to create a p-bit component directly on a chip, which allows for voltage-driven randomness. By running simulations of the circuit, they evaluated a p-bit design that uses three transistors and one MTJ, examining how each part influences the final output of the p-bit.

Paper [35] showcased p-bits built entirely on CMOS technology, utilizing the random threshold switching characteristic of a bistable n-p-n resistor, known as a biristor. The study confirmed the sigmoidal correlation between input and output by analyzing the digital signals from the biristor p-bits. It also successfully executed reversible Boolean logic functions. Moreover, the research solved a complex max-SAT problem, proving the method’s effectiveness in resolving concrete computational issues. The biristor p-bit not only consumes low power but also shows remarkable consistency in repeated operations and minimal variation between devices, thanks to its compatibility with standard commercial CMOS manufacturing processes. These advantageous traits suggest that biristor p-bits have the potential to overcome the constraints of traditional von Neumann architecture.

Reference [6] introduces a probabilistic autonomous data acquisition method that converts the stochastic response of a p-bit into a cognitive decision on whether to sample data. this approach uses a modified p-bit design with improved tunability, driven by an analog feature extraction circuit. Simulations from an active seismic

survey demonstrated the feasibility of lossless probabilistic data acquisition, achieving nearly 50% saving in both active operation time and the number of generated samples. The proposed design lacks the experimental implementation of the p-bit circuit. Additionally, the design could benefit from encryption since the acquired data signifies valuable information.

In general, the p-bit has proven to be useful in encoding probabilistic information, as demonstrated theoretically in the concept of probabilistic sensing. However, experimental demonstration is yet to be demonstrated. The fact that probabilistic sensing introduces a RNG in the circuit opens opportunities for various applications, such as in sensor encryption, which also have yet to be demonstrated experimentally.

2.3 In Sensor Data Encryption

A strong encryption algorithm is defined by two essential qualities: robust security and high speed. Since these algorithms are integrated into various applications such as e-banking, online shopping, and email services, they must operate quickly and maintain security across diverse platforms. Cryptography involves developing methods to ensure that information is transmitted securely from sender to receiver, even when third parties are present [36].

The research in [37] introduces an innovative algorithm that takes advantage of the reflective nature of balanced binary search trees to reduce extra work and uses a changing offset to enhance security significantly. When tested against well-known encryption methods like AES and DES, this new algorithm showed faster processing

times, used memory efficiently, and achieved a 50.1% rate of success in meeting the avalanche effect—a standard for encryption strength. Moreover, the variable nature of the offset was proven to be truly random, as it passed a battery of statistical tests set by the National Institute of Standards and Technology (NIST).

Reference [38] addresses the weaknesses of stream ciphers, such as poor linear complexity, issues with the clocking mechanism (majority rule), short clocking periods, weak choices of clocking taps, and collision problems. These vulnerabilities can allow intruders to decrypt stream ciphers. To enhance security, the proposed approach introduces a Non-Linear Feedback Shift Registers (NLFSRs), reuses 32 bits of SRES generated by the A3 algorithm, and combines the output stream with the last 32 bits of CGI. The randomness of the proposed stream cipher is analyzed using the NIST Statistical Test Suite. The results demonstrate a significant improvement in the randomness of the bit-stream, leading to enhanced security. The design shows passing 7 tests only out of 16 tests.

Reference [39] discusses the key expansion process for the Quantum Noise Random Stream Cipher (QNRC). The authors conducted NIST randomness tests on the extended key. Additionally, they proposed a new hash expansion algorithm that demonstrates higher efficiency in counter mode. The test results indicate that the extended key, generated using the AES and the hash function in counter mode, meets the randomness requirements. This approach ensures secure key usage while achieving efficient expansion. The design demonstrated the p-value only without mentioning the randomness condition.

In [40], the authors conducted a randomness analysis of a proposed cryptographic

Table 2.2: Comparison Between the Existing Encryption Algorithms.

Ref	Method used	Number of registers	Number of NIST Tests Passed	Processing time
[36]	Multiradix Trivium	3 Registers, 288 bits	-	-
[37]	Binary Search Trees	-	5	162-775ms
[38]	SRES Generated by A3	3 Registers, 114 bits	7	-
[39]	Hash Expansion Algorithm	1 Register, 256 bits	13	-
[40]	Modified Vernam Cipher	1 Register, 100 bits	4	-

algorithm that combines multilevel substitution and encryption techniques. They presented statistical test results using the NIST Statistical Test Suite to assess the randomness behavior of the keystream output. The statistical analysis included non-parametric test selections such as cumulative sums, runs tests, longest runs of ones, and frequency analysis. The experiment involved 100 samples, each with a length of 100 bits. The algorithm achieved an average success rate of 99.50% across the four statistical tests. Based on these results, it can be assumed that the proposed cryptographic algorithm effectively produces a random ciphertext sequence. For future work, the authors recommend implementing it in a software application to enhance the protection of electronic medical records. The design illustrated passing only 4 tests out of the 16 test in the NIST test suite.

In a summary the literature illustrates that a strong encryption method should contain 3 important aspects which are the methodology used, the processing time and the randomness of the generated keystream verified by the NIST test suite. ?? summarizes the mentioned aspects for each studied reference in data encryption section.

CHAPTER 3

RESEARCH GOALS

As mentioned earlier in the Introduction (Chapter 1), and highlighted later in the Literature Review (Chapter 2), the main goal of this thesis is to:

Design and Implement a Reliable Autonomous Data-Acquisition System with Embedded Security

In order to achieve this main research outcome, the following main research goals are identified as attributes that the system needs to achieve in its design:

1. Intelligence
2. Autonomy
3. Security

The details of these goals and the strategies set for achieving them are outlined in the upcoming three Sections, namely 3.1, 3.2 and 3.3, respectively.

3.1 Intelligence

3.1.1 Number of Features Captured

The chosen number of features are likely identified as providing the most relevant information for differentiating between event and non-event occurrence. These features are selected to capture significant characteristics that aid in accurate classification. Increasing the number of features significantly raises computational requirements. A balance is sought between capturing enough information for accurate classification while keeping the computational load manageable. Beyond a certain point, adding more features might not yield substantial gains in classification accuracy. The number of features chosen might represent a point where additional features provide diminishing returns in terms of improving the system's performance. Limiting the number of features also aids in practical implementation of hardware, reducing complexity, power consumption, and processing time. This choice aligns with the desired efficiency and performance trade-offs for specific systems

Accordingly, a single feature was able to provide a good degree of reliable probabilistic event detection [6][7]. However, to increase the reliability in the proposed autonomous data acquisition design, an additional feature, simple amplitude, was added. This addition does not burden the system with a high power budget while still enhancing its reliability and the performance.

3.1.2 Probabilistic Activation Instead of Deterministic

In power-hungry applications, such as remote sensors, wearable technology, and various IoT devices, sampling and data acquisition can consume significant amounts of power. This high-power consumption poses a challenge, especially for devices that rely on batteries or operate in environments where power sources are limited or recharging is infrequent. To address this, one innovative approach involves probabilistic activation of the system. This method activates data acquisition components based on the probability of event occurrence rather than on a fixed, deterministic schedule. Probabilistic activation increases the likelihood of avoiding the sampling of unwanted or redundant data. In deterministic systems, sensors may operate on a strict schedule, collecting data at regular intervals regardless of whether significant events are occurring. This often leads to the collection of large amounts of irrelevant or redundant data, wasting valuable power resources. For instance, a sensor monitoring environmental conditions might continue to sample data during periods of stability, even when no meaningful changes are occurring. By contrast, probabilistic activation allows the system to sample data in a more efficient manner. The system can dynamically adjust its average random sampling rate, increasing it during periods of higher event probability and reducing it when the likelihood of event-occurrence is low. This adaptive approach ensures that the system is more likely to capture relevant data, thereby conserving power by avoiding unnecessary sampling.

In this thesis, the strategy used to embed intelligence into the proposed autonomous data acquisition design is to adopt probabilistic activation in our system,

which will be implemented experimentally for the first time. Due to limited access to fabrication facilities for implementing the sMTJ devices, an emulation method using FPGA will be employed to emulate the response of the sMTJ in the p-bit.

3.2 Autonomy

3.2.1 Energy Efficiency

Conventional IoT sensors operate continuously to gather and analyze data, leading to significant inefficiencies in energy usage. The relentless, non-stop functioning of these sensors drains power resources, making them less efficient and sustainable, particularly for devices with limited battery life. The literature explores strategies aimed at reducing power consumption by shifting from a continuous operation model to an on-demand activation model. In this on-demand model, data collection and analysis components are only activated, when necessary, rather than operating all the time. By doing so, the system components remain in a low-power state until triggered by specific conditions or events that warrant data acquisition. This approach significantly conserves energy, as it eliminates the unnecessary power expenditure associated with constant operation. For instance, instead of continuously monitoring environmental conditions, a sensor might activate only when there is a change in the detected parameter beyond a predefined threshold. This selective activation reduces the frequency of data processing tasks, thereby extending the battery life of IoT devices and improving their overall efficiency. Additionally, the literature emphasizes the integration of smarter algorithms and adaptive mechanisms that can predict and

respond to environmental changes more accurately. These advanced techniques ensure that sensors are activated only when necessary, further optimizing energy use. By adopting these energy-efficient strategies, IoT systems can achieve a more sustainable operation, making them more viable for long-term applications in various fields such as environmental monitoring, smart homes, and industrial automation. This shift towards an on-demand model not only conserves energy but also enhances the longevity and reliability of IoT devices, providing a significant advancement in the field of sensor technology and data acquisition [41][42][43].

As mentioned before the probabilistic autonomous activation method reduces the sampling of unneeded information which in turn saves the overall power of the system. Additionally, a new element was added to enhance the power usage of the AFE block namely: clipping amplifiers, that reduces the power of the AFE circuit without compromising the rapid detection of the events.

3.2.2 Real-Time Event Detection

Rapid and accurate detection of relevant events in the analog domain is a major challenge. The research seeks to develop an analog-based event detection circuit capable of instantaneously recognizing specific features in the sensor signal. Any delay in the event detection process could lead to a significant time delay which is undesirable in autonomous data acquisition systems. The system must be accurately and precisely designed to meet such requirements. Most of the literature is focusing on reducing the power of the feature extraction unit while disregarding the importance of capturing the data in real-time.

3.2.3 Detection Delay

The processing power and speed of the hardware can impact detection times. If the hardware is not powerful enough or optimized for the specific task, it might take longer to process the data. Moreover, Noisy or variable signals might require more processing time to distinguish relevant information from background noise or fluctuations. The complexity of the event being detected can influence the detection time. Simple events might be recognized faster than complex or multi-stage events [44].

The goal of this thesis is to achieve real-time event detection which needs the onset detection delay to be less than the sampling interval of the sensor's signal. Many applications requires the onset detection delay to be in under the order of milliseconds (e.g., active seismic surveys) which require sampling interval to be less than 500 *us*. However, the aim here is to achieve a low as possible onset detection delay while incorporating the reduction of the power in the system.

3.3 Security

3.3.1 In Sensor Data Encryption

Encryption is a fundamental technique used to ensure that only authorized individuals or systems can access and read data, playing a crucial role in protecting sensitive information from unauthorized access and potential data breaches. By converting readable data into an unreadable format through cryptographic algorithms, encryption ensures that even if data is intercepted during transmission or accessed without

authorization, it remains incomprehensible to any malicious actor without the appropriate decryption key. One of the primary benefits of encryption is the protection it offers to sensitive data during transmission over networks. Whether data is being sent over the internet, through internal company networks, or via other communication channels, encryption acts as a robust shield against interception. This is especially important for personal data, financial information, and confidential business communications, which are frequent targets of cyber-attacks. Secure transmission protocols like HTTPS, which incorporate encryption, have become standard practice to safeguard data in transit [45]. In addition to protecting data in transit, encryption also maintains the integrity of data during storage. Data stored on devices, whether in databases, on hard drives, or in the cloud, is vulnerable to unauthorized access and tampering. Encryption ensures that even if someone gains physical or virtual access to the storage medium, the data remains protected. This layer of security is essential for maintaining confidentiality and integrity, ensuring that stored data cannot be read or altered without detection. Encryption also plays a critical role in ensuring data integrity. When data is encrypted, any tampering or unauthorized modification of the data can be detected because it will result in a failed decryption process. This characteristic of encryption makes it an effective tool for verifying that data remains unchanged during storage or transmission. For instance, encrypted messages in communication applications will not decrypt correctly if they are altered, alerting users to potential security issues. Moreover, by employing encryption, organizations can significantly mitigate the risks associated with data breaches and cyber-attacks. Data breaches can lead to severe financial losses, reputational damage, and legal conse-

quences for organizations. Encryption helps to reduce these risks by rendering stolen data useless to attackers. Even if cybercriminals manage to breach a system and exfiltrate data, the encrypted information will remain unreadable without the decryption key, thereby minimizing the impact of the breach [46].

To implement encryption effectively, organizations need to adopt comprehensive encryption strategies that cover data at rest and data in transit. This includes using strong encryption algorithms and key management practices to protect encryption keys. Organizations must ensure that encryption keys are stored securely and are not accessible to unauthorized individuals. Regularly updating encryption protocols and conducting security audits are also critical practices to address emerging threats and vulnerabilities [47].

In this thesis ciphering approaches that benefit from RNGs will be implemented to due the fact that implementation of p-bit already provides reliable RNG in the system, and this will be exploited in achieving in sensor encryption using ciphering techniques that utilises this RNG.

CHAPTER 4

MAIN CONTRIBUTIONS

The main contributions achieved in this work are highlighted below, categorized under the three main research domains highlighted earlier in the previous chapters, namely: (1) Analog Feature Extraction, (2) Probabilistic Sensing, and (3) In-Sensor Data Encryption. These three domains are covered in the upcoming three Sections, namely 4.1, 4.2 and 4.3, respectively.

4.1 Analog Feature Extraction

- Added an extra features (amplitude) to the real time event detection mechanism.
- Reduced the overall AFE power by 70% while still incorporating the new feature.

4.2 Probabilistic Sensing

- Implemented for the first time probabilistic autonomous data acquisition experimentally.

- Enhanced the overall power saving of the system from 69% ((Deterministic autonomous data acquisition)) to 93% ((Probabilistic autonomous data acquisition)) during active seismic events [6][7].

4.3 In Sensor Data Encryption

- Incorporated for the first time in sensor p-bit based data encryption.
- Experimentally demonstrated for the first-time stochastic sharing among two different p-bits driving two different applications; data acquisition and data encryption.

CHAPTER 5

SYSTEM DESIGN

To achieve the main goal of this thesis, the design and implementation of a reliable and secure autonomous data acquisition system, while ensuring the application of the primary research strategies discussed in Chapters 3 and 4, this chapter explains in detail the main components and techniques used to design such a system. The overall system architecture is described in Section 5.1, while the detailed system design is presented in Section 5.2.

5.1 Overall System Architecture

Figure 5.1 illustrates the overall system architecture. Additionally, the component-level system implementation is shown in Figure 5.2. The design comprises four main blocks: AFE unit, activation unit, data acquisition unit and encryption unit. When the geophone sensor captures seismic waves, the signal first enters the AFE block. For our specific application, the extracted features are the rate of change in the signal's amplitude and the amplitude itself. Subsequently, the extracted features will indicate

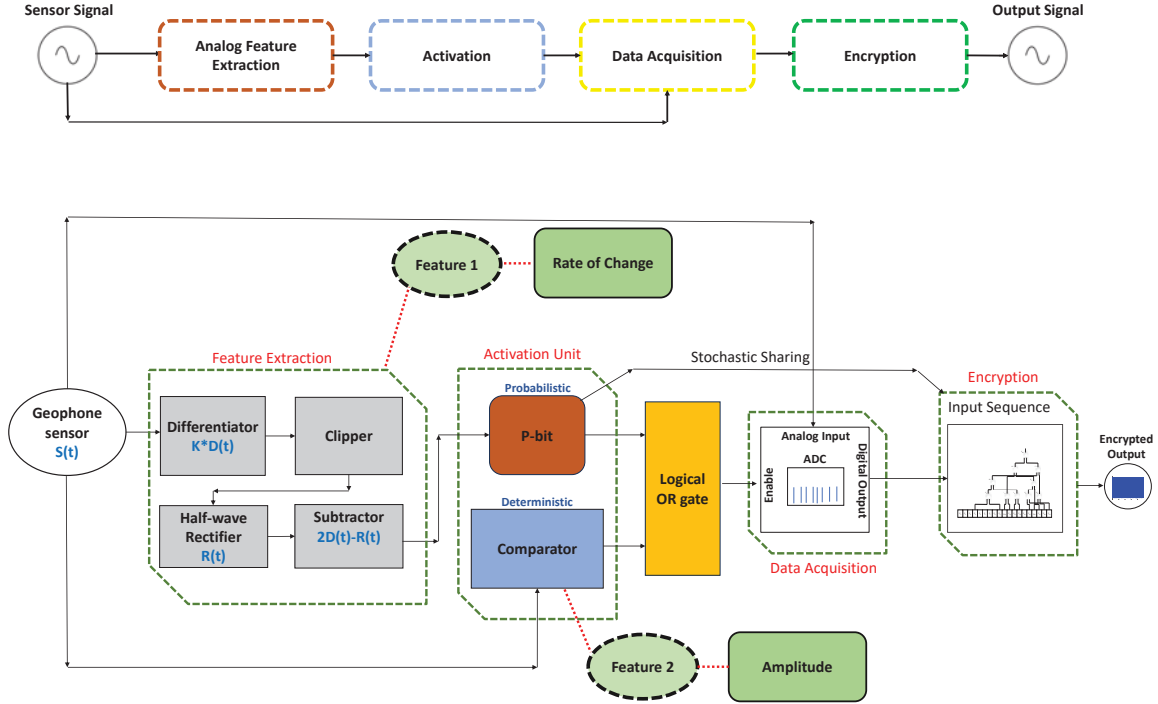


Figure 5.1: Block diagram demonstrating the over all system architecture including all the units (e.g., AFE unit, Activation unit, Data acquisition unit and Encryption unit).

the occurrence of an event, activating the second block, the activation unit. The system includes two activation schemes: probabilistic activation and deterministic activation. Probabilistic activation selectively triggers the data acquisition unit based on a certain level of confidence. It compares the AFE signal with the fluctuations of the SMTJ to determine whether to proceed with sampling or not. In the deterministic activation scheme, the actual signal amplitude is compared with a fixed threshold at which the presence of an event is confirmed, which then deterministically triggers the data acquisition unit. Additionally, the probabilistic and deterministic activation signals are combined using a logical OR gate, enabling the data acquisition unit to

plaintext.

5.2 Detailed System Design

This chapter further decomposes the architecture of the system mentioned in section 5.1 into 3 main blocks, namely: (1) Analog Feature Extraction, (2) Probabilistic Sensing, and (3) In-Sensor Data Encryption. The detailed design of each block is precisely explained in subsections 5.2.1, 5.2.2 and 5.2.3 respectively.

5.2.1 Analog Feature Extraction

The AFE circuit is composed of 3 main stages which are the differentiator, clipper and full wave rectifier as shown in Figure 5.2. The first stage, which is the Differentiator, computes an output signal by taking the time derivative of the sensor signal ($S(t)$) and scaling it by a gain factor (K). This resulting output, denoted as ($D(t)$), is then fed into a half-wave rectifier, which produces another signal called ($R(t)$). Next, the rectified signal ($R(t)$) is subtracted from twice the value of ($D(t)$) using the formula: ($2D(t) - R(t)$). The result of this subtraction is a full-wave rectified version of the differentiated signal ($D(t)$). Finally, this full-wave rectified output is supplied as an input to the probabilistic activation unit. The differentiator components are $Op - amp_1$, R_1 , R_2 , C_1 and C_2 . The transfer function of the differentiator is given by eq. 5.1

$$\frac{V_o}{V_I} = \frac{C_1 R_2}{s^2 R_1 R_2 C_1 C_2 + s(R_1 C_1 + R_2 C_2) + 1} \quad (5.1)$$

As this seems to be a simple ideal differentiation design, the low and high cutoff

frequencies are denoted by the following equations:

$$f_l = \frac{1}{2\pi C_1 R_1} \quad (5.2)$$

$$f_h = \frac{1}{2\pi C_2 R_2} \quad (5.3)$$

In our application, which involves capturing features of seismic waves from a geophone sensor, the targeted frequencies are very low, in the range of 10-100 Hz. It's important to emphasize that the operating frequency should be determined by the frequency of the input signal during an event, rather than the frequency at which the events occur. Prior to the third stage, which is the rectification stage the second stage will clip the differentiated signal from the absolute V_{DD} and V_{SS} to V_{clip1} and V_{clip2} . The purpose of the clipping is purely related to the power reduction of the circuit. It was observed that before clipping the differentiated signal, the rectification stage receives a high-amplitude signal, necessitating higher power for processing. However, after clipping the signal to a lower amplitude, the power required for rectification is significantly reduced. Subsequently, the clipper circuit consists of $Op - amp_2$, $Op - amp_3$, resistors R_3 , R_4 , diodes D_1 , D_2 . The third which is the rectifier stage includes $Op - amp_4$, $Op - amp_3$, resistors R_5 , R_6 , R_7 , and D_3 . $Op - amps_{6,7}$ are responsible for extracting the second feature, which is the amplitude of the signal. As the amplitude reaches the thresholds of V_{detr1} and V_{detr2} the data acquisition unit will be activated deterministically . The AFE circuit parameter values are as follows: $R_1 = 1 \text{ k}\Omega$, $R_2 = 500 \text{ k}\Omega$, $R_3 = R_4 = R_5 = R_7 = 5 \text{ k}\Omega$, $R_6 = 1 \text{ k}\Omega$, $C_1 = 0.33 \text{ uF}$, $C_2 = 10 \text{ pF}$.

5.2.2 Probabilistic Sensing

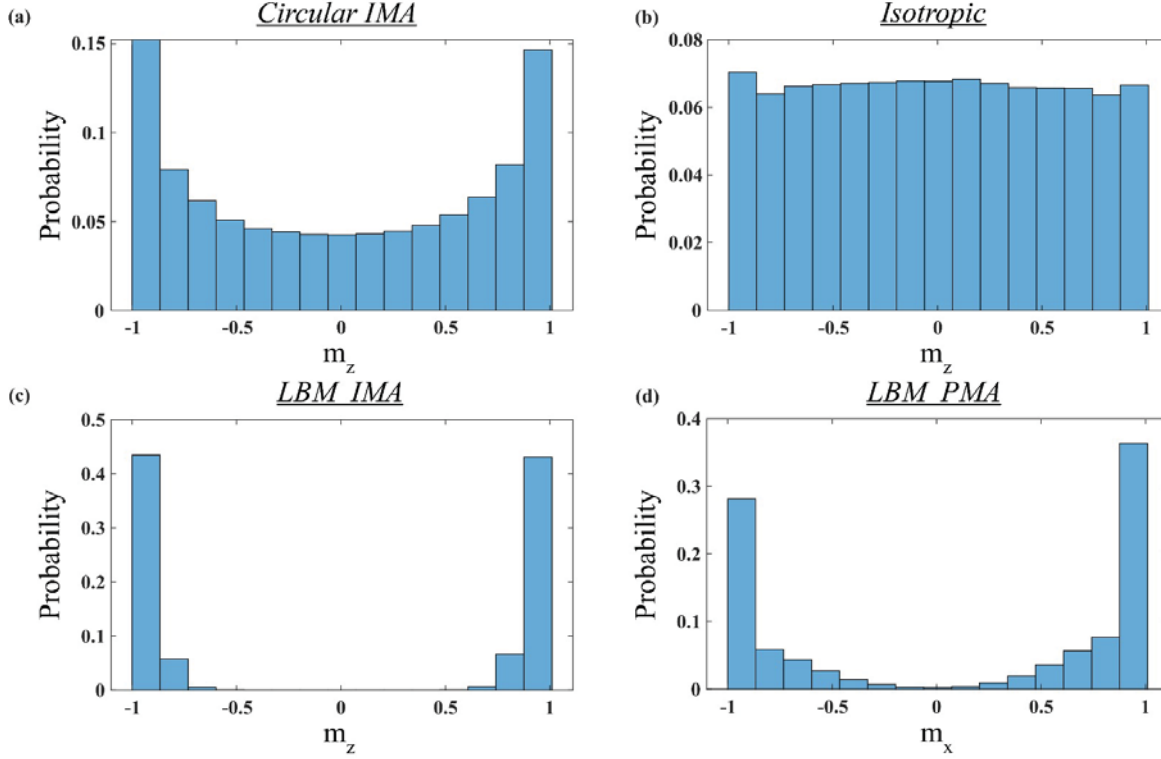


Figure 5.3: Magnet fluctuation dynamics for various types of magnets are analyzed. The simulations provide sample probability distributions of magnetization for: (a) a circular IMA, (b) an isotropic magnet, (c) a LBM with IMA, and (d) a LBM with PMA. [3].

The p-bit functions as a True Random Number Generator (TRNG). Its stochastic behavior and tunability makes it highly suitable for a wide range of applications. What sets the p-bit apart from a conventional RNG is its tunability. The stochasticity of the p-bit is driven by the sMTJ, enabling it to function as a RNG with controllable randomness. Figure 5.3 illustrated the different probability that could be achieved by employing different magnet types of the MTJ. The distribution is drastically changed with different magnet types. Nonetheless, the variance of the distribution gives the ability of the p-bit to serve in different applications. The simulation was conducted

using LTSPICE software, and the SPICE environment was integrated with MATLAB to model the stochastic dynamics of the p-bit. These dynamics are influenced by the magnetization state. To simulate the stochastic dynamics of the p-bit, the magnetization state $m_z(t)$ of the sMTJ was used. The conductance $G(t)$ of the sMTJ is defined as follows:

$$G(t) = G_0 \left[1 + \frac{m_z(t) \cdot \text{TMR}}{2 + \text{TMR}} \right] \quad (5.4)$$

where G_0 represent the average conductance, TMR is the tunneling magnetoresistance ratio that depends on the ratio between parallel resistance (R_p) and anti-parallel resistance (R_{AP}) of the MTJ defined as:

$$\text{TMR} = \frac{R_{AP} - R_P}{R_P} \quad (5.5)$$

MATLAB is employed to simulate the dynamic magnetization state $m_z(t)$ of the spin-transfer sMTJ and its associated probability distribution. The resulting $m_z(t)$ vector is then utilized to solve 5.4, yielding a time-varying vector $G(t)$. Subsequently, the SPICE simulation receives the sMTJ's response as a time-varying resistance based on $G(t)$. Notably, an isotropic magnet was chosen for the free layer due to its uniform $m_z(t)$ distribution [3]. The p-bit design utilized in our application comprises an NMOS transistor, resistor R8, a sMTJ, and an Op-amp. The comparator will assess the output of the AFE signal against the p-bit fluctuations from the MTJ to determine whether to activate the data acquisition, based on the likelihood of an event occurring. The results demonstrate that using p-bit-based activation significantly reduces power

consumption by minimizing the sampling of redundant data. Moreover, the p-bit output ORed with the output from the second feature will be connected to the enable port of the ADC to insure the sampling of only event information. For the first time it was experimentally proved that p-bit stochasticity sharing is possible where the p-bit will be sharing its stochasticity to produce the input of the encryption circuit .

5.2.3 In Sensor Data Encryption

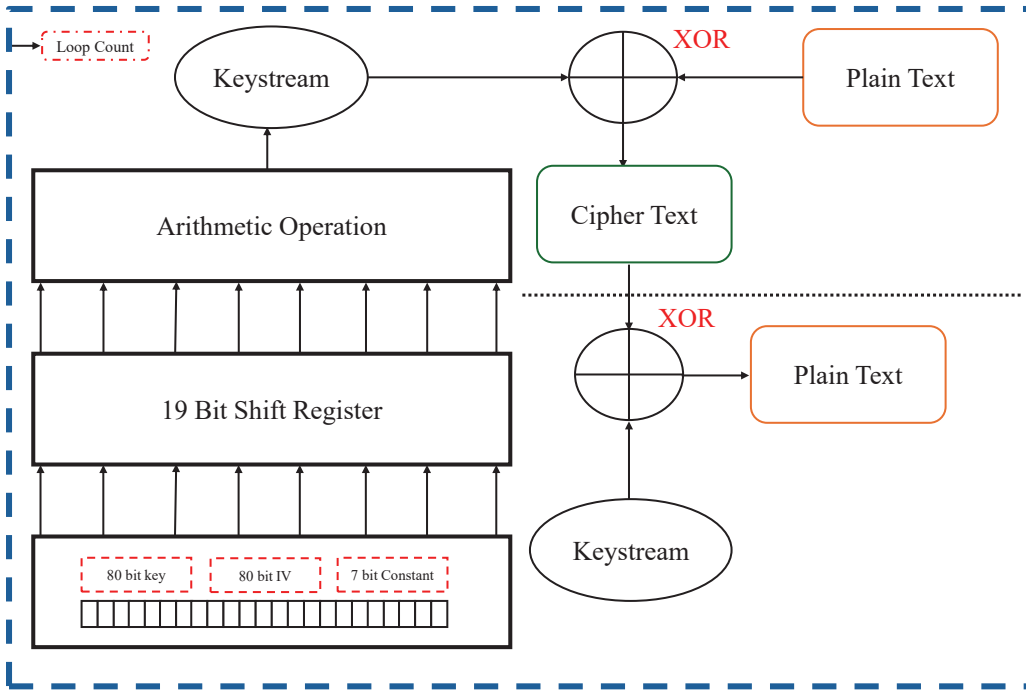


Figure 5.4: Proposed design Trivium stream cipher block diagram demonstrating the mechanism of how the key stream is developed and the operation to cipher the plain text message and deciphering it.

To ensure the security of data transmission, the reconstructed signal obtained from the ADC is encrypted using the Trivium ciphering method. Figure 5.4 demonstrates the working mechanism of the proposed Trivium method. First, the cipher circuit

requires an input which is driven for the p-bit consisting of three main components: the key, the Initialization Vector (IV), and a seven-bit constant. Moreover, the input will be inserted a 19-bit shift register that will shift the bits 1 time to the right each loop iteration. As the bits shift through the shift register, multiple Boolean operations are performed at each state to ensure a highly random sequence. A keystream will be generated after performing the Boolean operations and will be XORed with the plain text to produce the cipher message. Subsequently, the decrypted message will be obtained by XORing the cipher message with the keystream. This process will run for a fixed number of iterations to produce the keystream. For the receiver to decrypt the cipher text only the keystream and the ciphered text will be communicated.

CHAPTER 6

SYSTEM IMPLEMENTATION

After discussing the system design in the previous chapter, this chapter explains how the design of the p-bit and the modified Trivium ciphering method was implemented experimentally in the FPGA board, detailing the component level design of each block. Both the FPGA based p-bit and the modified Trivium ciphering circuit are explained in Sections 6.1 and 6.2 respectively.

6.1 Emulating the P-bit Behaviour in FPGA Board

It has been demonstrated in the literature that the p-bit can also be designed in a FPGA as in [48]. The FPGA implemented p-bit consists of 3 main blocks which are the Linear Feedback Shift Register (LFSR), activation function and comparator as shown in Figure 6.1. The LFSR functions as a customizable RNG, generating values from 0 to 1. The activation function is a sigmoid function, achieved by first applying the tanh function, then adding 1, and finally dividing the result by 2. An adjustment has been made to the FPGA-based p-bit design to shift the input values one position to the

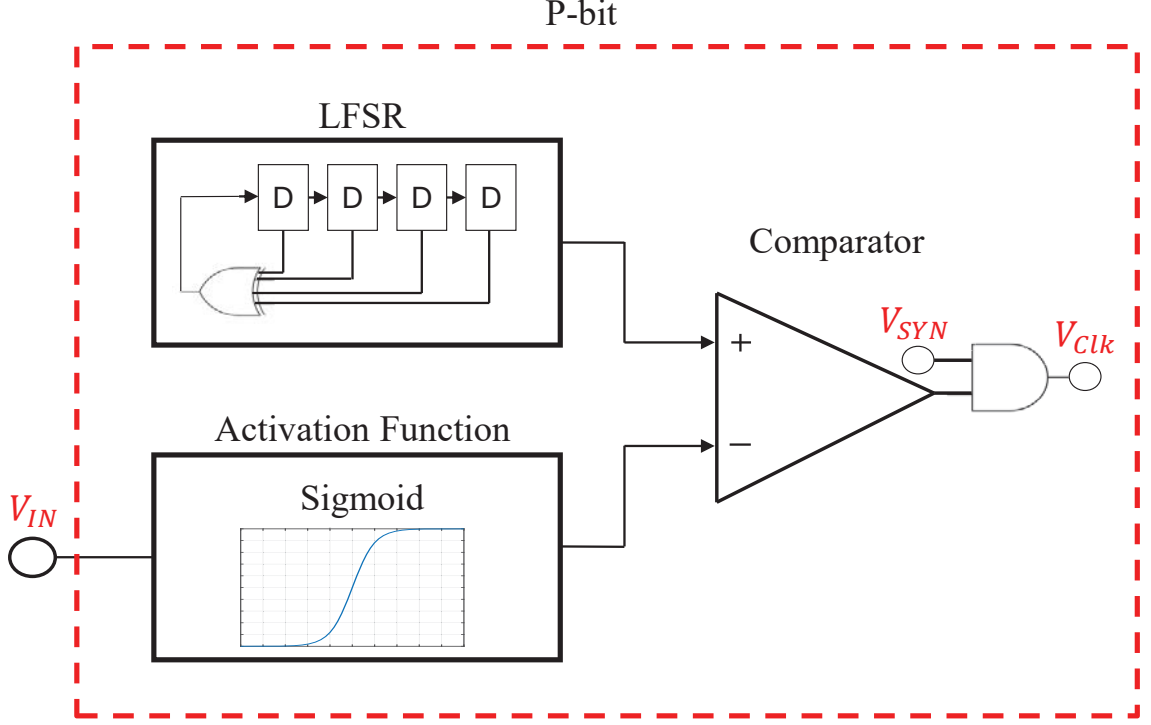


Figure 6.1: Proposed FPGA based p-bit design, showcasing the main blocks of the design, the output of the comparator is ANDed with a clock of 2000 samples per second.

left. This modification addresses the resultant values of the sigmoid function, where an input of 0 yields an output of 0.5, according to the specified sigmoid equation, which makes a false decision when the input of the AFE is 0 or close to 0. Thus, shifting the input is important to resolve this issue. During runtime, the input signal from the AFE is passed through the activation function, converting the AFE values to a range between 0 and 1. The comparator compares the output of the LFSR with the output of the activation function to determine whether to activate the data acquisition block. If the output of the AFE is greater than that of the LFSR, sampling will occur; otherwise, it will not. The primary advantage of the FPGA-based p-bit design over the one in [48] is its ability to accurately handle all values, including decimal points.

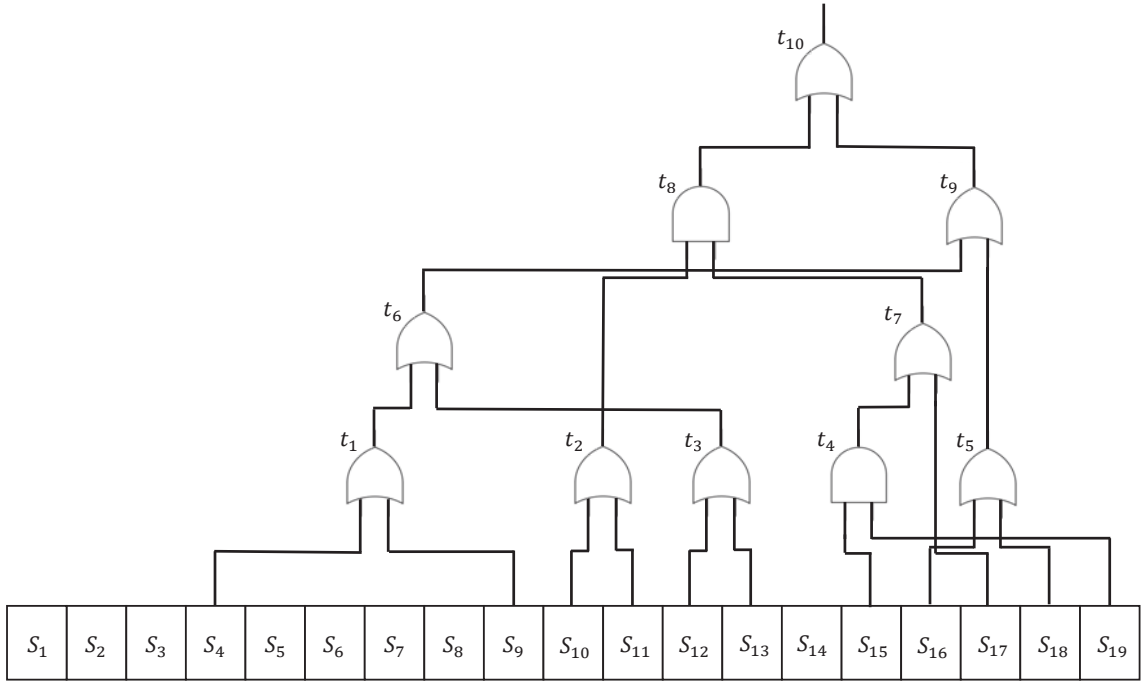


Figure 6.3: Component level implementation of the proposed modified Trivium stream cipher circuit design.

6.2 Proposed Trivium Circuit Design

Figure 6.3 illustrates the circuit implementation of the designed Trivium ciphering encryption. it is a novel approach that streamlines the encryption process while optimizing hardware utilization. Unlike the original Trivium encryption design, which employs multiple shift registers and a larger number of Boolean gates, this implementation utilizes a single shift register and a reduced number of gates, resulting in a more compact and efficient design.

One of the key features of this implementation is its integration with the data acquisition process. The ciphering occurs concurrently with data acquisition from the ADC, allowing for seamless encryption of data as it is being collected. This integration

minimizes processing overhead and ensures that sensitive information is encrypted in real-time, enhancing data security and confidentiality.

The core of the cipher circuit consists of a set of eight OR gates and two AND gates interconnected with each other. These gates are arranged in a specific configuration that enables the generation of a keystream used for encryption. The circuit operates in two nested loops: an inner loop that runs for 167 iterations and an outer loop that runs for 10,000 iterations. This arrangement results in the generation of a keystream with a length of 1,670,000 bits.

By utilizing a simplified circuit design and integrating encryption with data acquisition, this implementation offers several advantages. Firstly, it reduces the hardware footprint and power consumption compared to traditional Trivium implementations, making it suitable for resource-constrained environments. Secondly, the concurrent encryption and data acquisition enable real-time encryption of sensitive data, ensuring its security from the moment it is captured. Additionally, the streamlined design enhances overall system efficiency and performance, making it well-suited for applications requiring high-speed data processing and encryption. Eqs. 6.1-6.10 Describing the operations occurring within the Trivium circuit

$$S_4 \vee S_9 = t_1 \tag{6.1}$$

$$S_{10} \vee S_{11} = t_2 \tag{6.2}$$

$$S_{12} \vee S_{13} = t_3 \tag{6.3}$$

$$S_{15} \wedge S_{19} = t_4 \quad (6.4)$$

$$S_{16} \vee S_{19} = t_5 \quad (6.5)$$

$$t_1 \vee t_3 = t_6 \quad (6.6)$$

$$t_4 \vee S_{17} = t_7 \quad (6.7)$$

$$t_2 \wedge t_7 = t_8 \quad (6.8)$$

$$t_6 \vee t_5 = t_9 \quad (6.9)$$

$$t_8 \vee t_9 = t_{10} \quad (6.10)$$

The keystream generated from the ciphering circuit is the result of t_{10} generated from each iteration. Furthermore, the keystream along with the ciphered message will be transmitted to the receiver in order to decipher the message.

CHAPTER 7

RESULTS

This chapter describes the experimental setup used to test the implemented design discussed in Chapters 5 and 6. Additionally, the chapter presents the results obtained from the three main blocks of the system, which are the analog feature extraction, probabilistic sensing and in sensor data encryption units. The experimental setup followed by the results of these three main blocks are presented in Sections 7.1, 7.2, 7.3 and 7.4 respectively.

7.1 Experimental Setup

The full system was implemented both in experiment and simulation. LTC1051 Op-amp was used to build the AFE circuit in all blocks with a supply voltage of 3 V and -3 V as V_{DD} and V_{SS} . A SN74LS48N IC was used as the OR gate which performs ORing operation of the output from both positive and negative thresholding responsible for extracting the second feature. The p-bit was built by using MYRIO-1900 which contains an FPGA unit. The MYRIO-1900 was programmed and tested by

using LABVIEW environment. The encryption circuit was also implemented in the MYRIO-1900. The ADC used in the data acquisition unit to reconstruct the signals is AD4003 which is an 18-bit ADC with 1000k samples per second. The MYRIO-1900 encompasses both ADC and DAC in its analog input ports and analog output ports respectively. The ADC in the MYRIO-1900 is a 12-bit and has a sampling rate of 500k samples per second.

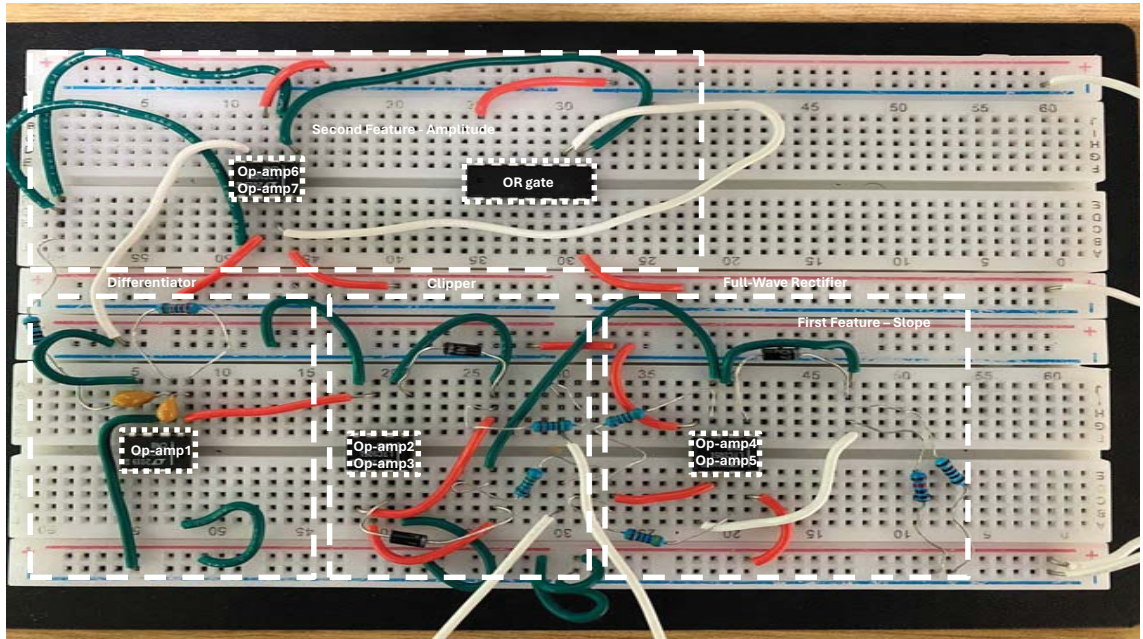


Figure 7.1: Experimental setup illustrating the AFE circuit with all of the stages and the interconnection between the IC's and the passive components.

The experimental setup of the AFE block along side the second feature block are demonstrated in Figure 7.1.

Figure 7.2 illustrates the complete system, showing the connection between the AFE unit and the FPGA-based p-bit. The first MYRIO-1900 device simultaneously handles probabilistic activation, encryption, and data acquisition. After extracting the first feature, which is the slope of the signal, the AFE output transmit this signal

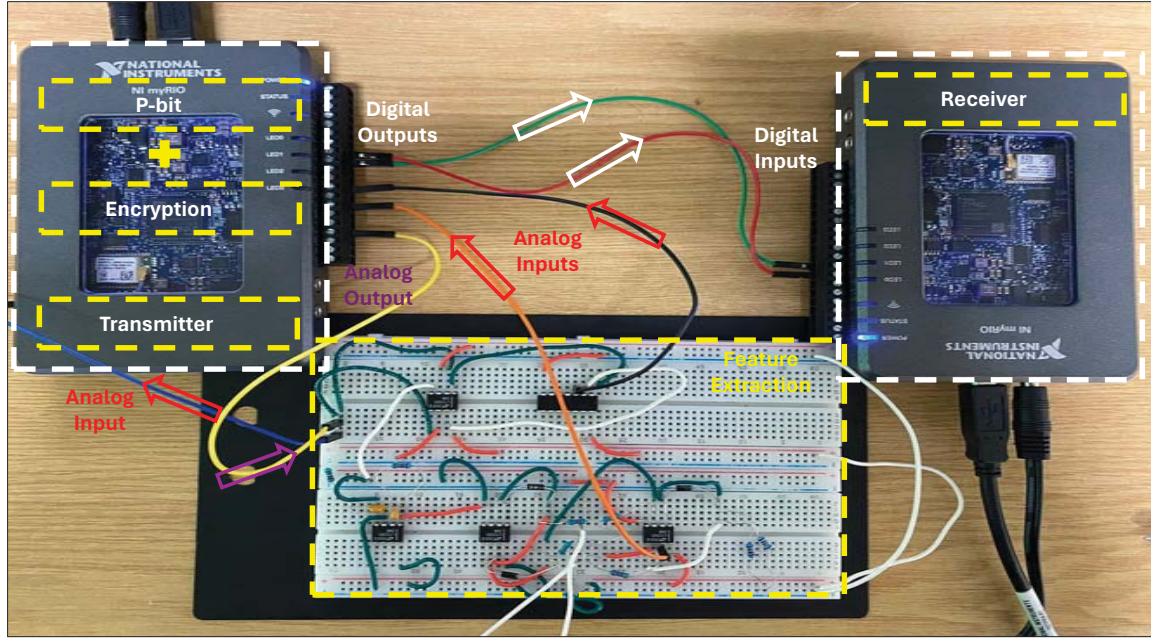


Figure 7.2: Experimental setup illustrating the AFE circuit and the MYRIO-1900 with the connections of the analog inputs and outputs as well as the digital inputs and outputs.

to the FPGA via port analog input C/AI0. This port allows the signal to be fed into the p-bit as an input to perform probabilistic activation. Moreover, the output signal from the OR gate, representing deterministic activation, is fed into the FPGA through analog input port C/AI1. This signal is then ANDed with the probabilistic activation to activate the data acquisition unit both probabilistically and deterministically. The original sensor signal, supplied as an input to the AFE circuit, is generated by the analog output port C/AO0. This signal passes through the AFE unit, which extracts its features and reconstructs the signal based on it. The original sensor signal is fed into the ADC via port A/AI1 and controlled by an enable signal from the activation unit. This ADC is responsible for reconstructing the output signal after extracting its features. Additionally, after encrypting the reconstructed signal, the first MYRIO-1900 on the left will act as the transmitter, sending both the keystream and the

encrypted signal to the receiver. The digital output port C/DO1 will transmit the keystream to the receiver, which will receive it via port C/DI1. The encrypted signal will be sent through port C/DO2 and received by the receiver through port C/DI2.

7.2 Analog Feature Extraction

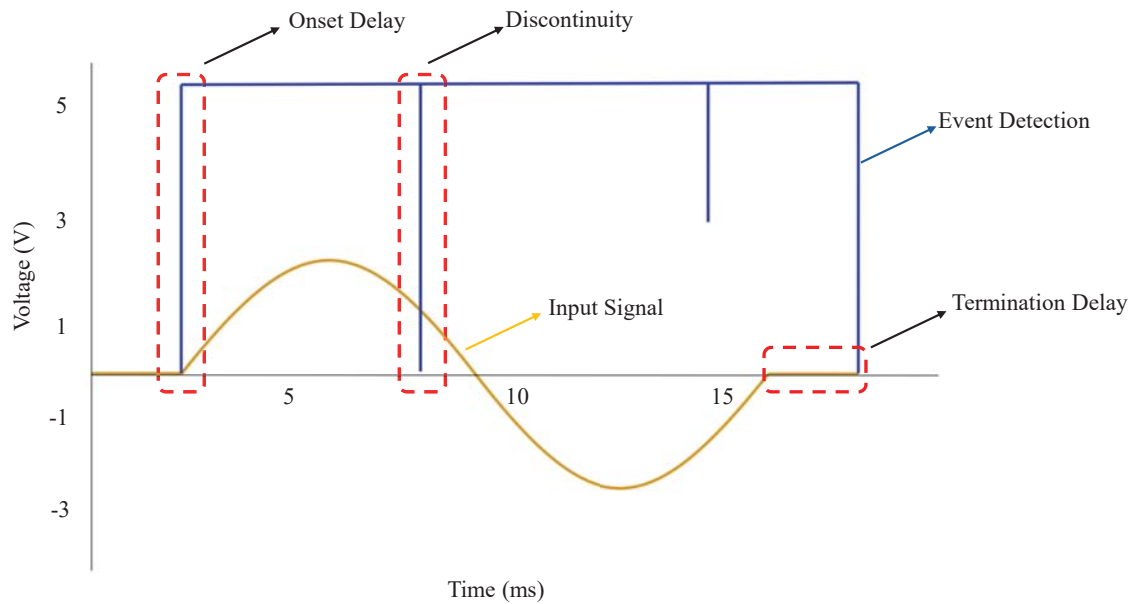


Figure 7.3: For a sine wave input to the AED, the blue curve depicts the nonideal behavior as determined by simulation. The red circles indicate regions where nonideal behavior is observed "Modified from [3]".

The idea of reducing the power comes with the consideration to maintaining a low detection delay, which means a fast system. The three main attributes shown in Figure 7.3"Modified from [3]" which are the detection delay, discontinuity and termination delay must be very low to achieve power optimization with acceptable speed that will enable autonomous data acquisition. Moreover, the onset delay stands

for the duration from the event's beginning to when the AFE circuit begins delivering a high output. This attribute must be very low to ensure high detection speed. The discontinuity occurs at the peaks and troughs where the slope is zero. This results in a discontinuity during the event because the differentiator outputs zero, which turns off the circuit. The termination delay is the duration from the event's ending to when the AFE circuit begins producing a low output, it preferable for this attribute to be little bit long to acquire some extra samples. Table 7.1 shows the measurement for these parameters of the original design compared to the proposed design. The results indicated that reducing the power of the AFE circuit did not increase these delays significantly. Thus, achieving on time data acquisition. The differentiated signal was clipped from 3 V and -3 V to 1 V and -1 V. The clipping of the differentiated signal resulted in less usage of power when entering the third stage which is the rectifying stage. As a result of clipping, the output of the AFE is reduced from the original 5 V to 1 V in the proposed design. To adjust the saturation level and ensure a fair comparison between the AFE output and the MTJ fluctuation level, the gain of the differentiator stage was reduced by decreasing the value of R_2 to 500k Ω . Additionally, The deterministic activation unit compares the input signal with threshold values of 100 mV and -100 mV (V_{detr1} and V_{detr2}). When the amplitude of the input signal reaches either of these thresholds, the signal is sampled immediately. These thresholds were chosen after studying a set of 23,000 seismic wave survey. This study included examining random events to determine when the AFE output reaches a maximum of 1 V, indicating the presence of an event. The survey included 230 geophone sensors with a total of 100 shots at multiple locations which results in a total of 23000 traces.

Table 7.1: Detection delay parameters and power consumption comparison between the original design and the proposed design.

Design	Onset delay	Discontinuity	Termination delay	Power consumption
Original	4.8 μs	4 μs	1.2597 ms	65 mW
Proposed Design	2.8 μs	1.7837 μs	1.26 ms	20 mW

Subsequently, all of the recored traces are composed of 4000 time samples with a total duration of 1 s [50].

7.3 Probabilistic Sensing

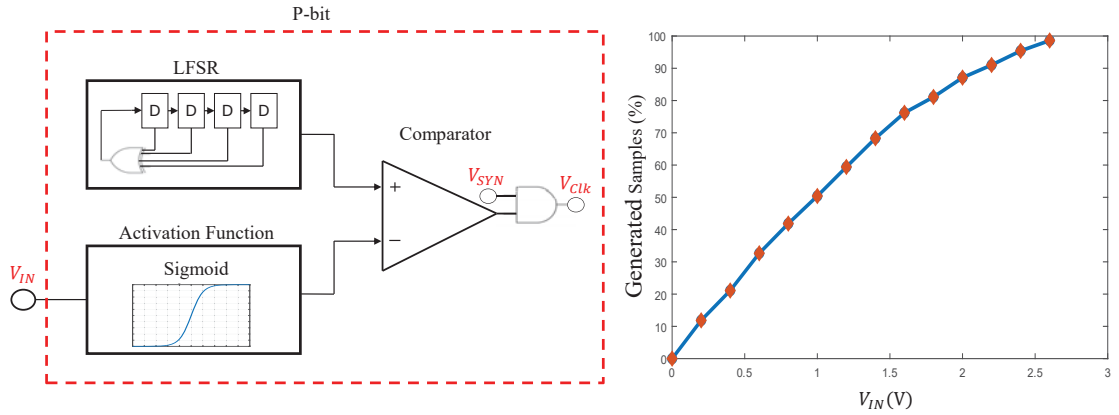


Figure 7.4: The percentage of generated samples by the probabilistic activation unit for different input voltages (V_{IN}).

To verify the functionality of the p-bit in experiments, a voltage versus generated sample measurement was conducted, as shown in Figure 7.4. The voltage level supplied to the activation function of the FPGA based p-bit was increased from 0 V to 3 V. The results indicate that as the input voltage increases, the number of generated samples also increases linearly.

The designed system was tested to assess how the slope of an input signal affects

the average random sampling rate triggered by the p-bit. To conduct this analysis, a triangular wave input signal with a constant absolute slope was employed. At each slope value the AFE yields an output voltage level which is compared with the fluctuation of the MTJ in simulations or the LFSR in experiment to give a number of samples based on the probability level. The Probabilistic Sensing circuit, depicted in Figure 6.2, revealed the following behavior: Input signals with very high slopes were continuously sampled, signals with very low slopes were disregarded a signal with intermediate slopes were sampled at a rate in relevance to their slope, as demonstrated in Figure 7.5. The clock associated with the p-bit is generating 2000 samples per second, in the analysis the percentage is computed in reference to the clock sample rate. Conducting this analysis is crucial to ensure low-slope events are properly captured while minimizing unnecessary data collection. This approach helps conserve the system's overall power.

In some scenarios, the sensor signal may not detect an event for an extended period. Conversely, in cases of high event occurrence, we can be certain that events are imminent. Based on these conditions, three modes were developed to capture features from events.

Relaxed Mode: This mode is activated when it is likely that no events will occur for a prolonged period. To best describe this mode, think about it as if we had a cup of tea, and we know the tea cold so we are relaxed to hold this cup while ensuring that our hands will not burn. Thus, we don't think about it as we want to take each sip of tea, our mind and senses are relaxed in this matter. Same goes for the proposed design where it can be modified to have a relaxed action saving more power in places

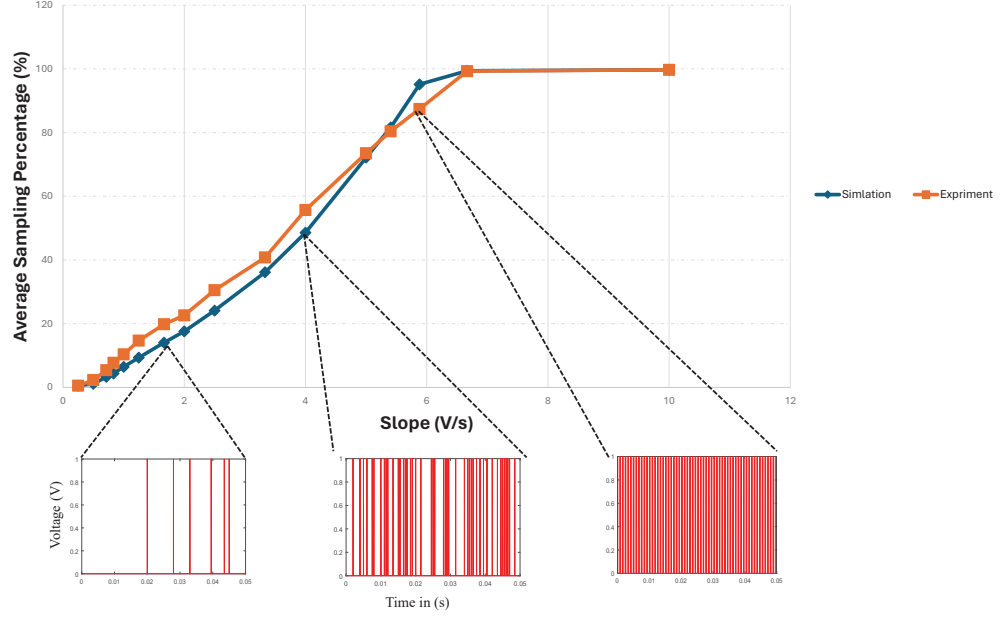


Figure 7.5: The average random sampling rate generated by the probabilistic activation unit vs slope. The projections at the bottom of the figure display transient output samples from the probabilistic activation unit for various data points on the curve corresponding to different slope values.

where it is known that an event will rarely be present.

Alert Mode: This mode is employed when we are certain that events will occur, necessitating to be prepared for sampling. Same goes for this mode, if we had a cup of tea which is very hot our senses will be more careful reminding us that the cup is hot and it will burn our hands. Thus, we will be more cautious as we want to take each sip of tea. In this mode the proposed design will have a high percentage sampling rate at low slopes to ensure acquiring the data in places of high event occurrence. This mode surely will consume more power but in turn will capture the data accurately.

Ideal Mode: This mode represents the system operating under normal conditions. The ideal mode is the standard at which the p-bit functions consistently across all locations.

Figure 7.6 illustrates the average sampling rate of the three developed modes. The average sampling is changed differently according to the mechanism of each mode. The results are verified from both experiment and simulations.

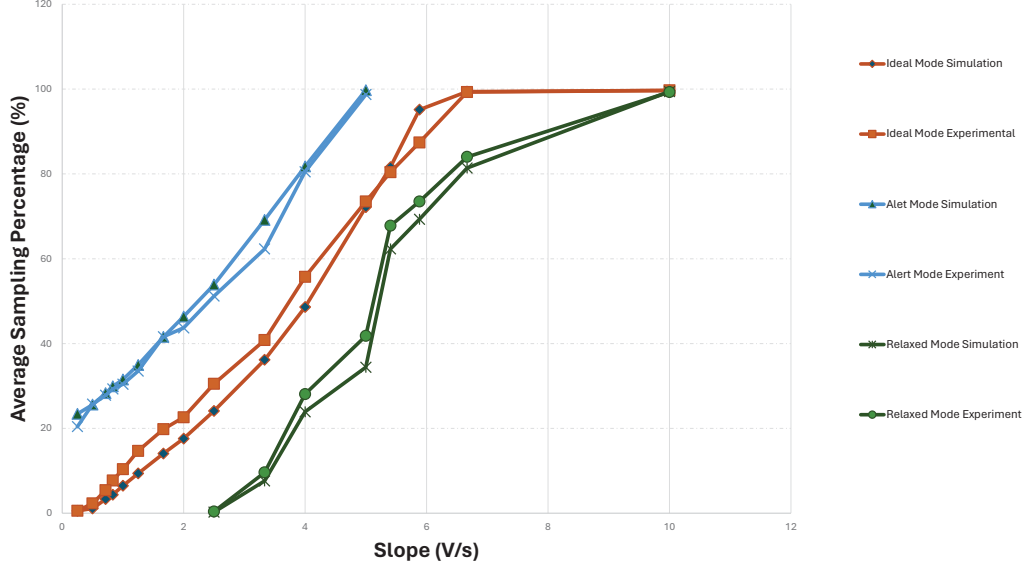


Figure 7.6: Average random generated samples vs slope demonstrated for the proposed modes of operation.

The various modes available are designed to enhance the efficiency of feature capture, which is contingent upon the anticipated event frequency. As depicted in Figure 7.7, the sampling behavior during an event is illustrated across three distinct scenarios. It is evident from the shown Figure 7.7 that the alert mode is characterized by a significantly higher sample rate, capturing the entire spectrum of the signal with utmost precision. This mode is particularly advantageous when the objective is to obtain a comprehensive dataset, ensuring that no critical information is missed. The ability to switch between modes ensures that the system remains adaptable to changing conditions and requirements, making it a versatile tool for a wide range of

applications.

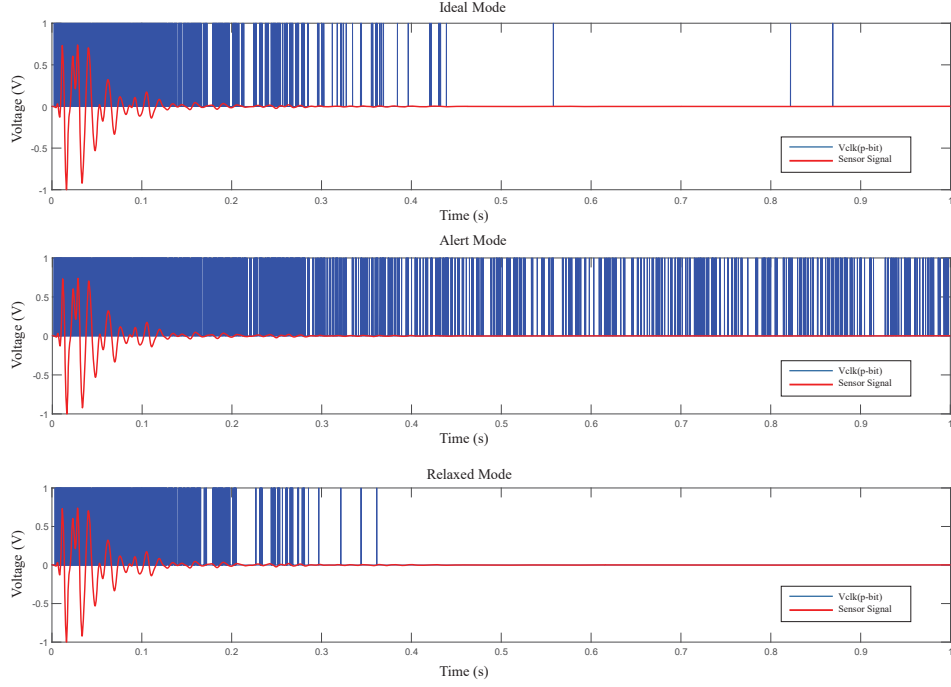


Figure 7.7: The behaviour of the sampling based on the mode of operation. Each mode was achieved by varying the value of V_{ref} in simulation, and varying the LFSR range in experiment.

7.4 In Sensor Data Encryption

Encryption occurs simultaneously as the reconstructed signal is acquired point by point. Each value of the reconstructed signal undergoes a conversion process from floating point to binary fixed-point representation within a loop. The 4000 samples acquired over time are transformed into a 32-bit binary fixed-point format and stored in an array consisting of 4000 rows and 32 columns. This array is then reshaped into a single row containing 128000 columns, housing all fixed-point numbers sequentially. This configuration enables the XOR operation with the keystream generated by the

Trivium encryption circuit, which produces a keystream consisting of 1,670,000 bits. Moreover, after XORing the values of the reconstructed signal with the keystream, a cipher signal will be produced. This cipher signal is XORed with the keystream to reproduce the original reconstructed signal. During the deciphering process, the array comprising 128,000 consecutive binary fixed-point numbers will be reshaped back into a structure of 4000 rows and 32 columns. This reshaped array then undergoes another loop to convert the fixed-point representation numbers back into floating-point numbers, which constitute the original reconstructed signal. To ensure the randomness of the keystream sequence generated by the Trivium circuit, 10 tests were conducted using the NIST test suite. This renowned suite assesses the randomness of sequences. The Trivium design successfully passed all 16 tests included in the suite. Table 7.2 displays these 16 tests and their p-values. A p-value close to 1 indicates a high likelihood of randomness, while a p-value close to 0 suggests a lower likelihood of randomness.

Table 7.2: NIST Test Suite Evaluation.

#	Test Name	P-Vale	Randomness	Success Rate
1	Frequency Test (Monobit)	0.33731788	Random	10/10
2	Frequency Test within a Block	0.45461815	Random	10/10
3	Run Test	0.42774534	Random	10/10
4	Longest Run of Ones in a Block	0.66527172	Random	10/10
5	Binary Matrix Rank Test	0.49389126	Random	10/10
6	Discrete Fourier Transform (Spectral) Test	0.55214319	Random	10/10
7	Non-Overlapping Template Matching Test	0.48461797	Random	10/10
8	Overlapping Template Matching Test	0.49543396	Random	10/10
9	Maurer's Universal Statistical test	0.43468837	Random	10/10
10	Linear Complexity Test	0.56191355	Random	10/10
11	Serial test	0.56751999	Random	10/10
12	Approximate Entropy Test	0.52914379	Random	10/10
13	Cumulative Sums (Forward) Test	0.400060282	Random	10/10
14	Cumulative Sums (Reverse) Test	0.371915894	Random	10/10
15	Random Excursions Test	0.519523879	Random	10/10
16	Random Excursions Variant Test	0.451627842	Random	10/10

To evaluate the accuracy of data acquired through the proposed probabilistic sensing approach, the entire data acquisition system was simulated three times: once

using a regular continuous sampling ADC (Regular ADC) and once using deterministic sampling ADC and (Deterministic ADC) Probabilistic Sensing system with an ADC enabled by a p-bit (Probabilistic ADC) [6][7]. The data collected by all of the systems—one operating in continuous sampling mode, one operating in deterministic sampling mode and the other in probabilistic sampling mode—were compared. Reconstructed signals for 50 different active seismic events were then analyzed. Furthermore, to accurately quantify all schemes, the reconstructed signals were compared with the original signal of 50 events and evaluated by using the Normalized Mean Squared Error (NMSE) as shown in eq. 7.1.

$$\frac{\|X_{Signal} - X_{ADC}\|_2^2}{\|X_{Signal}\|_2^2} \quad (7.1)$$

Where $\|\cdot\|_2$ is the second norm of a vector a , X_{Signal} is the original signal vector and X_{ADC} is the reconstructed signal by the three schemes ADC's.

Table 7.3 and Table 7.4 showcase the error values for all schemes along with the percentage of sample savings for both experiment and simulation. Experimental values closely align with simulation results. For the regular ADC, the experimental error is slightly higher due to the MYRIO-1900's sampling rate of 500k samples per second, compared to the 1000k samples per second used in the simulation. Nevertheless, the probabilistic ADC achieves a significant sample saving of 93%, which greatly enhances power efficiency in the data acquisition block.

Table 7.3: Experiment NSME Values with Sample Saving.

	Time	Freq 2000	Freq 200	Sampling Saving
ADC	7.74E-3	4.2E-3	5.3E-3	0
P-ADC	1.69E-2	5.3E-3	4.1E-3	93%
DADC	2.8E-2	2.2E-3	8.3E-3	69.575%

Table 7.4: Simulation NMSE Values with Sample Saving.

	Time	Freq2000	Freq200	Sampling Saving
ADC	1.5E-2	9.369E-6	4.336E-5	0
P-ADC	1.95E-2	7.5E-3	5.9E-3	91.64%
DADC	1.29E-2	2.4619E-4	4.5323E-5	76.295%

CHAPTER 8

DISCUSSION AND FUTURE WORK

8.1 Discussion

As demonstrated through Table 7.3 and Table 7.4 the probabilistic autonomous data acquisition was achieved with very low NMSE which means the acquisition was lossless and the error was insignificant. However, there was a big saving in the operation time of the system resulting much better performance than the deterministic autonomous data acquisition and this is only for the duration where there was an active seismic event taken place, if the duration's where there was no active seismic events to be taken to account the saving could reach up to 99%. On the other hand the proposed system was able to reduce the power consumption of the AFE circuit down by 70% while still using discrete components and increasing the number of features, this method proves that there is much more potential going forward in further reducing the over all power consumption of this block through more optimisation as well as going to integrated

design.

The demonstration of p-bit sharing amongst multiple applications opens avenues to achieving compact systems that share resources specifically in the most critical part in any probabilistic system which is the stochastic unit of the p-bit. Moreover, looking at the results of the encryption system in Table 7.2, a very compact implementation of Trivium ciphering technique was able to pass all the test of the NIST test suite showing high level of randomness for the cipher text and proving robustness in encryption and immunity to potential attacks. Nonetheless, there could be an opportunity of integrate both digital and analog parts into a single chip.

This probabilistic sensing after demonstrating it experimentally can be used in various applications such as in seismic data, biomedical wearable devices and monitoring systems etc.

The capability of tuning the stochastic unit of the p-bit in probabilistic sensing has shown its ability to be used in different applications depending on the frequency of an event occurring, as demonstrated in Figure 7.7 the p-bit can be employed and tuned according to the requirements of the application, offering the flexibility to choose between different modes of operation. This opens up vast opportunities for diverse event-based applications.

8.2 Future Work

The p-bit design can be implemented in a compact very efficient way that employs sMTJ as a discrete component on the same discrete level design with the rest of

the digital and the analog systems, as a first step it could be implemented in an Application-Specific Integrated Circuit (ASIC) custom design that connects the AFE unit and the digital unit which has the p-bit activation unit and the encryption unit. However, later on the system can be implemented as an integrated SoC combining all the units in single chip that would significantly reduce the power consumption and the size of the system.

The proposed design only showcases the use of two features which are the slope and the amplitude. However, the employment of additional features seems feasible and could enhance the system design further more achieving high accuracy in distinguishing the events of the sensor signal. Furthermore, there's no limitations or restrictions on the methods used to reduce the power consumption of the AFE block, many certain techniques could be used to further enhance the power efficiency of the AFE block.

CHAPTER 9

CONCLUSION

This thesis introduces several innovative optimizations and contributions to the concept of autonomous data acquisition, focusing on the implementation and experimentation of probabilistic autonomous data acquisition. For the first time, probabilistic sensing have been successfully implemented in an experimental setup using an FPGA board that emulates the behaviour of the p-bit, achieving results similar to those from simulations with sMTJ. Furthermore, the concept of p-bit sharing is demonstrated experimentally, which facilitates two distinct applications: probabilistic sensing and data encryption. The inherent stochasticity of p-bits is utilized to generate input sequences for the encryption unit, leading to the creation of a novel, power-efficient modified Trivium ciphering circuit using FPGA board, requiring fewer gates and a single shift register.

Additionally, an enhancement to the design was implemented by incorporating a second feature, ensuring deterministic sampling at high amplitudes. The use of clipper circuit resulted in a 70% reduction in the power consumption of the feature extraction unit. Overall, shifting from deterministic to probabilistic autonomous data acquisition

significantly improved system power savings, reducing it from 69% to 93% during active seismic events. This power reduction was achieved without compromising the system's speed, allowing for real-time autonomous data acquisition.

Achieving such accuracy with an enhanced, energy-efficient probabilistic autonomous data acquisition system opens the door to numerous applications. For instance, it can significantly impact very low-power IoT systems, enabling widespread deployment in smart homes, cities, and industries where long battery life is crucial. Wearable devices can benefit significantly, offering extended battery ranges that enhance user experience and reliability, especially in health and monitoring systems. Biomedical devices, particularly those designed to detect very low-frequency range signals, can achieve higher precision and longer operational times, improving patient outcomes and facilitating continuous health monitoring. Additionally, environmental and structural monitoring systems can leverage this technology to provide real-time data collection and analysis while conserving energy, making it feasible to deploy sensors in remote or hard-to-access locations. Overall, the advancements in probabilistic autonomous data acquisition pave the way for innovative, energy-efficient solutions across diverse fields, ensuring improved performance and sustainability.

APPENDIX A

SUPPLEMENTARY MATERIAL

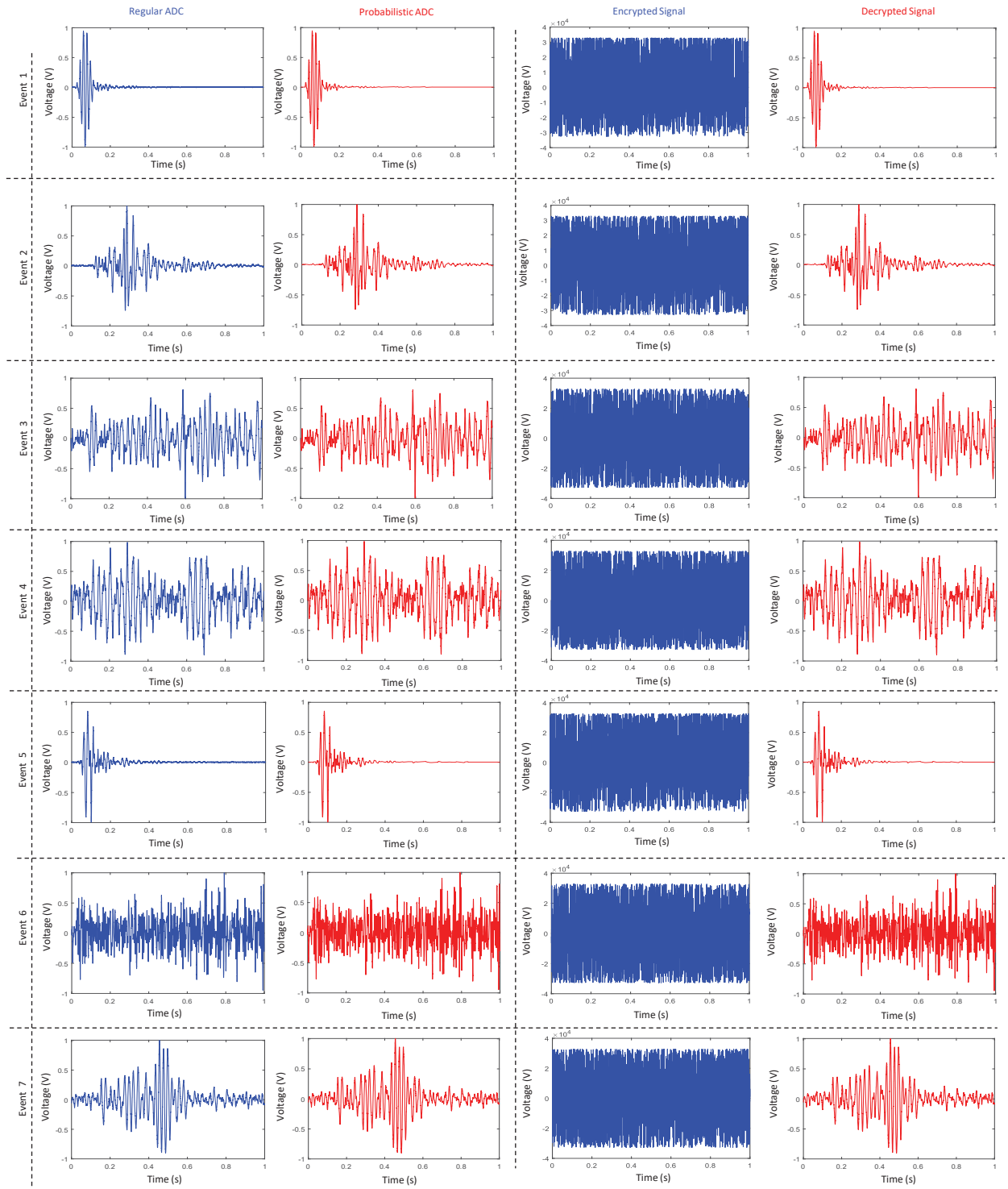


Figure A.1: Results for the probabilistic autonomous data acquisition and in sensor encryption part 1, events 1 - 7.

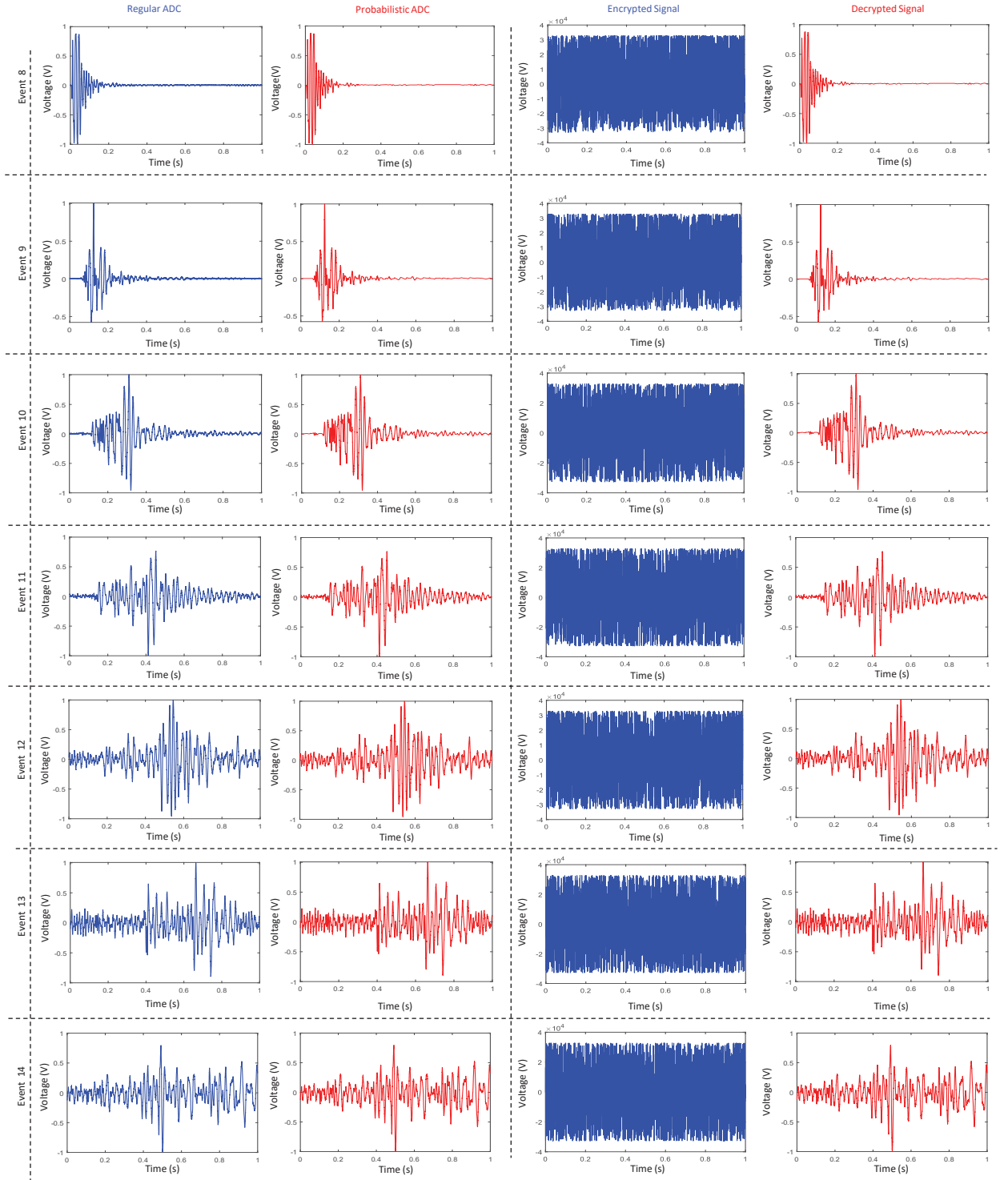


Figure A.2: Results for the probabilistic autonomous data acquisition and in sensor encryption part 2, events 8 - 14.

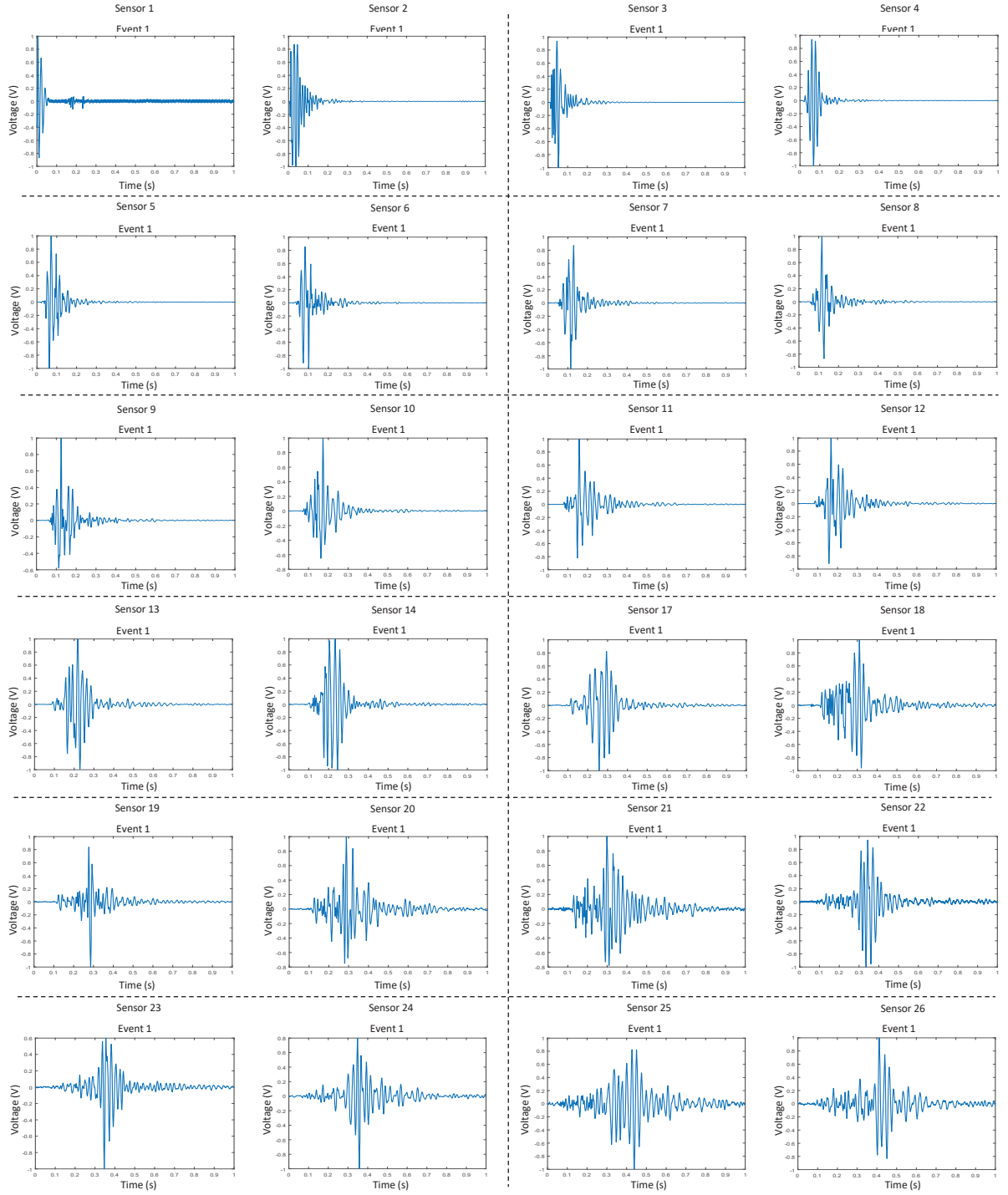


Figure A.3: Results for the 50 events used to calculate the NMSE part 1, events 1 - 24



Figure A.4: Results for the 50 events used to calculate the NMSE part 2, events 25 - 48

REFERENCES

- [1] S. Mourrane, B. Larras, A. Cathelin, and A. Frappé, “Event-driven continuous-time feature extraction for ultra low-power audio keyword spotting,” in *2021 IEEE 3rd International Conference on Artificial Intelligence Circuits and Systems (AICAS)*. IEEE, 2021, pp. 1–4.
- [2] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, “Iot architecture challenges and issues: Lack of standardization,” in *2016 Future Technologies Conference (FTC)*, 2016, pp. 731–738.
- [3] S. Bunaiyan and F. Al-Dirini, “Neuro-inspired autonomous data acquisition for energy-constrained iot sensors,” *IEEE Sensors Journal*, vol. 22, no. 20, pp. 19 466–19 479, 2022.
- [4] G. Gallego, T. Delbrück, G. Orchard, C. Bartolozzi, B. Taba, A. Censi, S. Leutenegger, A. J. Davison, J. Conradt, K. Daniilidis, and D. Scaramuzza, “Event-based vision: A survey,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 1, pp. 154–180, 2022.
- [5] T. Stoffregen, G. Gallego, T. Drummond, L. Kleeman, and D. Scaramuzza, “Event-based motion segmentation by motion compensation,” in *2019*

- IEEE/CVF International Conference on Computer Vision (ICCV)*, 2019, pp. 7243–7252.
- [6] S. Bunaiyan and F. Al-Dirini, “Probabilistic autonomous data acquisition using stochastic mtj based p-bits,” in *2024 8th IEEE Electron Devices Technology Manufacturing Conference (EDTM)*, 2024, pp. 1–3.
- [7] —, “Real-time analog event-detection for event-based synchronous sampling of sparse sensor signals,” in *2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*. IEEE, 2021, pp. 1053–1057.
- [8] M. Gazivoda and V. Bilas, “Always-on sparse event wake-up detectors: A review,” *IEEE Sensors Journal*, vol. 22, no. 9, pp. 8313–8326, 2022.
- [9] J. Van Assche and G. Gielen, “Power efficiency comparison of event-driven and fixed-rate signal conversion and compression for biomedical applications,” *IEEE Transactions on Biomedical Circuits and Systems*, vol. 14, no. 4, pp. 746–756, 2020.
- [10] J. Kaiser and S. Datta, “Probabilistic computing with p-bits,” *Applied Physics Letters*, vol. 119, no. 15, 2021.
- [11] V. S. Shetty, R. Anusha, D. Kumar M.J., and P. Hegde N., “A survey on performance analysis of block cipher algorithms,” in *2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020, pp. 167–174.

- [12] C. D. Cannière, “Trivium: A stream cipher construction inspired by block cipher design principles,” in *Information Security Conference*, 2006. [Online]. Available: <https://api.semanticscholar.org/CorpusID:3812479>
- [13] A. Name. (2020) The estream portfolio page. [Online]. Available: <http://www.ecrypt.eu.org/stream>
- [14] B. K and S. G. Shiva, “Man-in-the-middle attack explainer for fog computing using soft actor critic q-learning approach,” in *2022 IEEE World AI IoT Congress (AIIoT)*, 2022, pp. 100–105.
- [15] H. Yu, K. He, C. Ling, Y. Liu, D. Chen, and T. Su, “A $2.81\mu\text{W}$, energy efficient mfcc feature extractor for keyword-spotting in 65nm cmos,” in *2023 8th International Conference on Computer and Communication Systems (ICCCS)*, 2023, pp. 56–61.
- [16] F. Chen, K.-F. Un, W.-H. Yu, P.-I. Mak, and R. P. Martins, “Design and implementation of a low power switched-capacitor-based analog feature extractor for voice keyword spotting,” in *2022 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, 2022, pp. 1–5.
- [17] H. Fuketa, “Ultralow power feature extractor using switched-capacitor-based bandpass filter, max operator, and neural network processor for keyword spotting,” *IEEE Solid-State Circuits Letters*, vol. 5, pp. 82–85, 2022.
- [18] S. Zhang, F. Su, Y. Wang, S. Mai, K. P. Pun, and X. Tang, “A low-power keyword spotting system with high-order passive switched-capacitor bandpass filters for

- analog-mfcc feature extraction,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 70, no. 11, pp. 4235–4248, 2023.
- [19] S. Ray and P. R. Kinget, “Ultra-low-power and compact-area analog audio feature extraction based on time-mode analog filterbank interpolation and time-mode analog rectification,” *IEEE Journal of Solid-State Circuits*, vol. 58, no. 4, pp. 1025–1036, 2023.
- [20] K. M. H. Badami, S. Lauwereins, W. Meert, and M. Verhelst, “A 90 nm cmos, 6 w power-proportional acoustic sensing frontend for voice activity detection,” *IEEE Journal of Solid-State Circuits*, vol. 51, no. 1, pp. 291–302, 2016.
- [21] F. Chen, K.-F. Un, W.-H. Yu, P.-I. Mak, and R. P. Martins, “A 108nm 0.8mm² analog voice activity detector (vad) featuring a time-domain cnn as a programmable feature extractor and a sparsity-aware computational scheme in 28nm cmos,” in *2022 IEEE International Solid-State Circuits Conference (ISSCC)*, vol. 65, 2022, pp. 1–3.
- [22] M. Kavishwar, P. Kurrey, and R. Zele, “Analog acoustic feature extraction and delta-sigma modulation based neural network classification for voice activity detection,” in *2022 IEEE 19th India Council International Conference (INDICON)*, 2022, pp. 1–4.
- [23] M. Cho, S. Oh, Z. Shi, J. Lim, Y. Kim, S. Jeong, Y. Chen, D. Blaauw, H.-S. Kim, and D. Sylvester, “17.2 a 142nm voice and acoustic activity detection chip for mm-scale sensor nodes using time-interleaved mixer-based frequency scanning,”

- in *2019 IEEE International Solid-State Circuits Conference - (ISSCC)*, 2019, pp. 278–280.
- [24] M. Croce, B. Friend, F. Nesta, L. Crespi, P. Malcovati, and A. Baschiroto, “A 760 nw, 180 nm cmos analog voice activity detection system,” in *2020 IEEE Custom Integrated Circuits Conference (CICC)*, 2020, pp. 1–4.
- [25] U. Mukherjee, T. Halder, A. Kannan, S. Ghosh, and S. Pavan, “A 28.5 μ w all-analog voice-activity detector,” in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2021, pp. 1–5.
- [26] E. Shi, X. Tang, and K. P. Pun, “A 270 nw switched-capacitor acoustic feature extractor for always-on voice activity detection,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 3, pp. 1045–1054, 2021.
- [27] N. Goux, J.-B. Casanova, G. Pillonnet, and F. Badets, “A 6-nw 0.0013-mm² ilo bandpass filter for time-based feature extraction,” *IEEE Solid-State Circuits Letters*, vol. 3, pp. 306–309, 2020.
- [28] J. S. P. Giraldo, S. Lauwereins, K. Badami, and M. Verhelst, “Vocell: A 65-nm speech-triggered wake-up soc for 10- μ w keyword spotting and speaker verification,” *IEEE Journal of Solid-State Circuits*, vol. 55, no. 4, pp. 868–878, 2020.
- [29] T. Tekeste, H. Saleh, B. Mohammad, A. Khandoker, and M. Ismail, “A nano-watt ecg feature extraction engine in 65-nm technology,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 8, pp. 1099–1103, 2018.

- [30] Y. Lv, R. P. Bloom, and J.-P. Wang, “Experimental demonstration of probabilistic spin logic by magnetic tunnel junctions,” *IEEE Magnetics Letters*, vol. 10, pp. 1–5, 2019.
- [31] K. Y. Camsari, S. Salahuddin, and S. Datta, “Implementing p-bits with embedded mtj,” *IEEE Electron Device Letters*, vol. 38, no. 12, pp. 1767–1770, 2017.
- [32] J. L. Drobitch and S. Bandyopadhyay, “Reliability and scalability of p-bits implemented with low energy barrier nanomagnets,” *IEEE Magnetics Letters*, vol. 10, pp. 1–4, 2019.
- [33] S. Bunaiyan and F. Al-Dirini, “Mtj-based p-bit designs for enhanced tunability,” in *2022 IEEE Nanotechnology Materials and Devices Conference (NMDC)*, 2022, pp. 14–16.
- [34] J. Daniel, Z. Sun, X. Zhang, Y. Tan, N. Dilley, Z. Chen, and J. Appenzeller, “Experimental demonstration of an on-chip p-bit core based on stochastic magnetic tunnel junctions and 2d mos2 transistors,” *Nature Communications*, vol. 15, no. 1, p. 4098, 2024.
- [35] J. Kim, J.-K. Han, H.-Y. Maeng, J. Han, J. W. Jeon, Y. H. Jang, K. S. Woo, Y.-K. Choi, and C. S. Hwang, “Fully cmos-based p-bits with a bistable resistor for probabilistic computing,” *Advanced Functional Materials*, p. 2307935, 2024.
- [36] J. M. Mora-Gutiérrez, C. J. Jiménez-Fernández, and M. Valencia-Barrero, “Multiradix trivium implementations for low-power iot hardware,” *IEEE Transactions*

- on *Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 12, pp. 3401–3405, 2017.
- [37] B. Alabdullah, N. Beloff, and M. White, “E-art: A new encryption algorithm based on the reflection of binary search tree,” *Cryptography*, vol. 5, no. 1, p. 4, 2021.
- [38] R. P. Prajapat, R. Bhadada, and G. Sharma, “Implementation of enhanced a5/1 stream cipher and its randomness analysis by nist test suite,” in *2021 IEEE International Symposium on Smart Electronic Systems (iSES)*. IEEE, 2021, pp. 426–431.
- [39] H. Shi, T. Pu, W. Mou, and Y. Chen, “Nist randomness tests on the extended key of quantum noise random stream cipher,” in *2019 18th International Conference on Optical Communications and Networks (ICOON)*. IEEE, 2019, pp. 1–3.
- [40] D. G. Brosas, A. M. Sison, A. A. Hernandez, and R. P. Medina, “Analysis of the randomness performance of the proposed stream cipher based cryptographic algorithm,” in *2020 11th IEEE Control and System Graduate Research Colloquium (ICSGRC)*. IEEE, 2020, pp. 76–81.
- [41] U. Singh and I. Chana, “Enhancing energy efficiency in iot (internet of thing) based application,” in *Inventive Computation Technologies 4*. Springer, 2020, pp. 161–173.

- [42] V. Reddy, M. Rabbani, M. T. Arif, and A. M. Oo, “Iot for energy efficiency and demand management,” in *2019 29th Australasian Universities Power Engineering Conference (AUPEC)*. IEEE, 2019, pp. 1–6.
- [43] W. B. Qaim, A. Ometov, A. Molinaro, I. Lener, C. Campolo, E. S. Lohan, and J. Nurmi, “Towards energy efficiency in the internet of wearable things: A systematic review,” *IEEE Access*, vol. 8, pp. 175 412–175 435, 2020.
- [44] M. Fedoryszak, B. Frederick, V. Rajaram, and C. Zhong, “Real-time event detection on social data streams,” in *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining*, 2019, pp. 2774–2782.
- [45] K. M. Hosny, M. A. Zaki, N. A. Lashin, M. M. Fouda, and H. M. Hamza, “Multimedia security using encryption: A survey,” *IEEE Access*, 2023.
- [46] B. Shao, T. Wan, F. Liao, B. J. Kim, J. Chen, J. Guo, S. Ma, J.-H. Ahn, and Y. Chai, “Highly trustworthy in-sensor cryptography for image encryption and authentication,” *ACS nano*, vol. 17, no. 11, pp. 10 291–10 299, 2023.
- [47] X. Ma, C. Wang, W. Qiu, and F. Yu, “A fast hyperchaotic image encryption scheme,” *International Journal of Bifurcation and Chaos*, vol. 33, no. 05, p. 2350061, 2023.
- [48] A. Z. Pervaiz, B. M. Sutton, L. A. Ghantasala, and K. Y. Camsari, “Weighted p -bits for fpga implementation of probabilistic circuits,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 6, pp. 1920–1926, 2019.

- [49] B. Altinoz and D. Unsal, “Look up table implementation for imu error compensation algorithm,” in *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, 2014, pp. 259–261.
- [50] U. T. . M. C. (UTAM). (2018) Seismic data library seismic data library. [Online]. Available: <http://utam.gg.utah.edu/SeismicData/SeismicData.htm>

VITAE

- Name: Ibrahim Abdulrahman Hussain Al-bulushi
- Nationality: Bulushi Resident
- Date of Birth: 7th of Jan 1994
- Email: *albulushiibrahim@gmail.com*
- Permenant Address: Iskan Al-Sharfyah, Toba St. , P.O. Box 3051, Postal Code 23217, Building No. 6147, Jeddah, Kingdom of Saudi Arabia.

- **Education:**

2021 - 2024: Master of Science in Electrical Engineering, King Fahd University of Petroleum and Minerals(KFUPM).

2015 - 2020 : Bachelor of Science in Electrical Engineering, Islamic University of Madinah (IUM).

- **Biography:**

Ibrahim Al-Bulushi received the B.Sc.degree (First Hons.) in electrical engineering from Islamic University of Madinah (IUM), Madinah, Kingdom of Saudi

Arabia, in 2020, where he is currently pursuing the master degree. He is currently a master student in Electrical Engineering, KFUPM, since 2020. His current research interests include event-based data acquisition, intelligent sensing, electric circuits, FPGA, probabilistic circuits and probabilistic bits (p-bit).

- **Publications:**

1 - Uzair, M., Al-Kafrawi, S., Al-Janadi, K., Al-Bulushi, I. (2022). A low-cost, real-time rooftop IoT-based photovoltaic (PV) system for energy management and home automation. *Energy Engineering*, 119(1), 83-101.

2 - Uzair, M., Yacoub Al-Kafrawi, S., Manaf Al-Janadi, K., Abdulrahman Al-Bulushi, I. (2022). A low-cost IoT based buildings management system (BMS) using arduino mega 2560 and raspberry pi 4 for smart monitoring and automation. *International journal of electrical and computer engineering systems*, 13(3), 219-236.