# Low power secured communication protocol in Wireless Body Area Networks

Junchao Wang
Supervisor: Prof. Zeljko Zilic

Doctor of Philosophy

Department of Electrical and Computer Engineering

McGill University

Montreal,Quebec

2019-05-06

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of Doctor of Philosophy

## DEDICATION

*To my lovely fiancée* ***Jing Liu*** *for her love, companionship, and support. To my parents* ***Dr. Jianping Wang*** & ***Ms. Ling Du*** *for their selfless and unconditional love and support.*

## ACKNOWLEDGEMENTS

First of all, I would like to express my gratitude and thanks to my supervisor ***Dr. Zeljko Zilic*** for his guidance, support, and encouragement. Without his knowledge, expertise, and commentary, it would have been extremely difficult to complete my Ph.D. program and dissertation.

Meanwhile, I would like to thank the ***China Scholarship Council*** and ***McGill University*** for the financial support of my Ph.D. program. I would not have such stable research and living environment without sufficient financial support from them.

Furthermore, I would like to thank my current colleagues who are also my cherished friends, ***Anastasios Alexandridis***, ***Amirhossein Shahshahani***, ***Ashraf Suyyagh***, and ***Farimah Poursafaei*** for the help they gave me in my life and research in the years we spent together in the laboratory.

In addition, I would like to express my sincere thanks to ***Kaining Han*** from the University of Electronic Science and Technology of China, who was a visiting student from September 2017 to September 2018 in the Department of Electrical and Computer Engineering at McGill University, for the efforts he put in our cooperation research projects.

Finally, I would like to give my deepest appreciation to my dearest parents, ***Dr. Jianping Wang*** and ***Ms. Ling Du***, who have devoted their life to my growth and education, always stood by me and sacrificed so much for me. Also, my sincere gratitude goes out to my beloved fiancée **Jing Liu** for her love, patience, and especially the company for the last eight years.

## ABSTRACT

With the rapid growth of the aging population in the world, it is quite challenging for the inefficient conventional medical and healthcare system to address the huge demands of medical services. Fortunately, the development of advanced biomedical sensors and wireless communication technology makes it possible to establish an eHealthcare system which supports all stages of care for the patients including prevention, diagnosis, treatment, and follow up remotely all day long.

In recent years, the concept of Wireless Body Area Networks (WBANs) has attracted significant interest in academic and industrial areas. WBANs specify the networks dedicated to the wireless communication of personal biomedical data between advanced sensors and centralized devices that are then used for health and lifestyle purpose. Compared to the prevailing wireless communication technologies such as Bluetooth and Zigbee, WBANs have the advantages of ultra-low power consumption, high reliability, and high-security protection while transmitting sensitive personal biomedical data. Meanwhile, benefiting from advanced biomedical sensors, multiple types of biomedical data can be collected relatively accurate from human beings. Therefore, the cooperation between WBANs and advanced biomedical sensors is a potential solution for continuously remote health condition monitoring for medical services, which is essential for addressing the larger medical demands caused by the trend of population aging.

In 2012, the 802.15.6 WBANs standard was released by the Institute of Electrical and Electronics Engineers (IEEE) to regulate the specifications of the communication in WBANs. However, even though WBANs have demonstrated multiple advantages in various perspectives, there are still some facts limiting the development of WBANs. For instance, the lack of complete and efficient baseband processing Application-Specific Integrated Circuit (ASIC) for WBANs makes it difficult to establish the actual communication networks for WBANs.

The general objective of the dissertation is to facilitate the emergence of eHealth-care systems with the low power and high-security WBAN systems performing on the patients' side, and a trusted health data transmission and storage system running in the back-end. Concretely, this dissertation proposes ASIC solutions which completely meet the requirements of PHY and security scheme specified in the IEEE 802.15.6 WBANs standard for the front-end. Also, a blockchain-based data exchange and storage system for WBANs is proposed for the back-end. In addition, to evaluate various designs in WBANs, the dissertation develops a unified evaluation platform for WBAN systems. In summary, we make a required step for the development of WBANs, especially for the low power ASIC designs for WBANs protocol. Meanwhile, the blockchain-based data exchange and storage system for WBANs provides a feasible solution for trusted medical data management for modern medical institutions.

# ABRÉGÉ

Avec la croissance rapide du vieillissement de la population dans le monde, il est très difficile pour le système de santé et de soins de santé conventionnel de répondre aux demandes énormes des services médicaux. Heureusement, le développement de capteurs biomédicaux avancés et de technologies de communication sans fil permet de mettre en place un système de cybersanté prenant en charge toutes les étapes de la prise en charge des patients: prévention, diagnostic, traitement et suivi à distance tout au long de la journée.

Au cours des dernières années, le concept de réseaux de zones de corps sans fil (WBAN) a suscité un vif intérêt dans les domaines académiques et industriels. Les réseaux WBAN spécifient les réseaux dédiés à la communication sans fil de données biomédicales personnelles entre des capteurs avancés et des périphériques centralisés, qui sont ensuite utilisés à des fins de santé et de style de vie. Comparés aux technologies de communication sans fil dominantes telles que Bluetooth et Zigbee, les réseaux WBAN présentent les avantages suivants: consommation d'énergie extrêmement basse, fiabilité élevée et protection hautement sécurisée lors de la transmission de données biomédicales personnelles sensibles. Parallèlement, grâce aux capteurs biomédicaux avancés, de nombreux types de données biomédicales peuvent être collectés de manière relativement précise auprès d'êtres humains. Par conséquent, la coopération entre les réseaux WBAN et des capteurs biomédicaux avancés constitue une solution potentielle pour la surveillance continue de l'état

de santé des services médicaux, ce qui est essentiel pour faire face aux demandes médicales plus importantes résultant du vieillissement de la population.

En 2012, la norme 802.15.6 WBAN a été publiée par l'Institut des ingénieurs électriciens et électroniciens (IEEE) afin de réglementer les spécifications de la communication dans les réseaux WBAN. Cependant, même si les WBAN ont démontré de multiples avantages dans diverses perspectives, certains faits limitent encore le développement de ces réseaux. Par exemple, le manque d'ASIC de traitement de bande de base complet et efficace pour les réseaux WBAN rend difficile l'établissement des réseaux de communication réels pour les réseaux WBAN.

L'objectif général de la thèse est de faciliter l'émergence de systèmes de cybersanté dotés des systèmes WBAN de faible puissance et de haute sécurité fonctionnant du côté des patients, ainsi que d'un système sécurisé de transmission et de stockage des données de santé. Concrètement, cette thèse propose des solutions ASIC qui répondent parfaitement aux exigences du PHY et du schéma de sécurité spécifié dans la norme IEEE 802.15.6 WBAN pour le frontal. En outre, un système d'échange et de stockage de données basé sur une chaîne de blocs pour les réseaux WBAN a été proposé pour le back-end. En outre, afin d'évaluer différentes conceptions dans les réseaux WBAN, la thèse proposait une plate-forme d'évaluation unifiée pour les systèmes WBAN. En résumé, les travaux effectués ont constitué une étape importante dans le développement des réseaux WBAN, en particulier pour les conceptions d'ASIC basse consommation pour le protocole WBAN. Parallèlement, le

système d'échange et de stockage de données basé sur une chaîne de blocs pour les réseaux WBAN constitue une solution réalisable pour une gestion fiable des données médicales dans les établissements médicaux modernes.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

## LIST OF ABBREVIATION

5G: Fifth Generation of Cellular Mobile Communication

ADC: Analog to Digital Converter

AES-CTR: Counter Operation Mode of AES

AES: Advanced Encryption Standard

ALM: adaptive Logic Module

API: Application Program Interface

ASIC: Application-Specific Integrated Circuit

AWGN: Additive White Gaussian Noise

BCH: Bose–Chaudhuri–Hocquenghem

BER: Bit Error Rate

BLE: Bluetooth Low Energy

BLER: Block Error Rate

CA: Certificate Authority

CCA: Clear Channel Assessment

CIHI: Canadian Institution for Health Information

CMC: Canadian Microelectronics Cooperation

CMOS: Complementary Metal-Oxide-Semiconductor

CRC-4: Cyclic Redundancy Check 4

D8PSK: Differential Eight Phase Shift Keying

DAC: Digital Analog Converter

DBPSK: Differential Binary Phase Shift Keying

DDC: Digital Down Converter

DES: Data Encryption Standard

DLT: Distributed Ledger Technology

DPSK: Differential Phase Shift Keying

DQPSK: Differential Quadrature Phase Shift Keying

DSA: Digital Signature Algorithm

DSP: digital signal processor

DSPs: Digital Signal Processing Units

ECC: Elliptic Curve Cryptography

ECDH: Elliptic-Curve Diffie-Hellman

ECDLP: Elliptic Curve Discrete Logarithm Problem

ECG: Electrocardiography

EEG: Electroencephalogram

EHRs: Electronic Health Records

ELP: Error Location Polynomial

FCS: Frame Check Sequence

FDTD: Finite-Difference Time-Domain

FPGA: Field-Programmable Gate Array

GDP: Gross Domestic Product

HBC: Human Body Communication

HCS: header check sequence

HDD: Hard-Decision Decoder

HMAC: Hash-based Message Authentication Code

IC: Integrated Circuit

IEEE: Institute of Electrical and Electronics Engineers

KVP: Key-Value Pair

LFSR: Linear Feedback Shift Register

LNA: Low Noise Amplifier

LTE: Long Term Evolution

LUT: Look-up-Table

MAC: Medium Access Control

MCU: Microcontroller Unit

MF: Medium Frequency

MICS: Medical Implant Communication Service

MIT: Massachusetts Institute of Technology

ML: Maximum Likelihood

MVCC: MultiVersion Concurrency Control

NB: Narrowband

NDS: Noise-Dependent Scaling

NIST: National Institute of Standards and Technology

NPCR: Number of Pixels Change Rate

PHY: Physical Layer

PLCP: PHY Convergence Protocol

PoS: Proof of Stake

PoW: Proof of Work

PPDU: Protocol Data Unit

PSDU: PHY Service Data Unit

RAM: Random-access memory

REST: Representational State Transfer

RF: Radio Frequency

RNE: Random Number Engine

ROM: Read-only memory

RSA: Rivest, Shamir, and Adelman

SDD: Soft-Decision Decoder

SDR: Software Defined Radio

SHA-256: Secure Hash Algorithm-256

SMIC: Semiconductor Manufacturing International Corporation

SNR: Signal to Noise Power Ratio

SNR: Signal-to-Noise Ratio

SoC: Systems on a Chip

SPA: Simple Power Analysis

SPI: Serial Peripheral Interface

SRRC: Square-Root Raised Cosine

SS: Scrambler Seed

UACI: Unified Average Changing Intensity

UI: User Interface

UML: Unified Modeling Language

UWB: Ultrawide-band

WBANs: Wireless Body Area Networks

WPANs: Wireless Personal Area Networks

# CHAPTER 1
# Introduction

This chapter introduces the dissertation in general including the motivation and context of the dissertation, introduction to the Wireless Body Area Networks (WBANs), the objectives of the research, the contributions of the dissertation, and the organization of the dissertation.

## 1.1 Motivation and context

As predicted by the International Data Base of U.S. Census Bureau [46] by 2037, twenty percent of the population in the United States and Canada will be aged over 65. Meanwhile, the number of people with chronic conditions in the world increased from approximately 118 million to 149 million in the past 25 years, while the number will increase to 171 million according to the prediction in [19]. In addition, according to the data provided by the Canadian Institution for Health Information (CIHI), the average health expenditure for every individual in Canada is $6,604$ Canadian dollars in 2017. It requires 11.5% of the overall Gross Domestic Product (GDP), up from only 7% of the GDP in 1975. In other words, the Canadians spent 60.8% more for healthcare over the past 43 years [17]. Even though the population required regular medical consulting is increasing and the money each individual in Canada spent in healthcare is rising as well, people still need to wait a long time before they can actually have medical services since the queues to consult medical professionals are getting longer due to the shortage of medical professionals; in Canada, for instance,

the average waiting time for healthcare queues was 21.2 weeks in 2017, as reported by the Fraser Institute [10]. Therefore, there is a strong demand for an efficient, economical, and secure healthcare system, which can not only monitor the physical conditions of the patients remotely but can also provide the feedback to the patients in different circumstances all day long.

With the rapid development of modern technology, especially the advanced wireless communication technologies and networks, eHealthcare systems could provide the means to address such a demand. By utilizing modern biomedical sensors, various types of networks, and cloud storage, an eHealthcare system can support all stages of care for the patients, including prevention, diagnosis, treatment, and follow up remotely [41]. As demonstrated in Figure 1–1, an eHealthcare system contains two major parts: the front-end and back-end. The front-end supports the communication between the biomedical sensors and centralized devices around the patients. The back-end is responsible for providing different types of medical services remotely and managing the medical data. The front-end and back-end are connected by public networks.

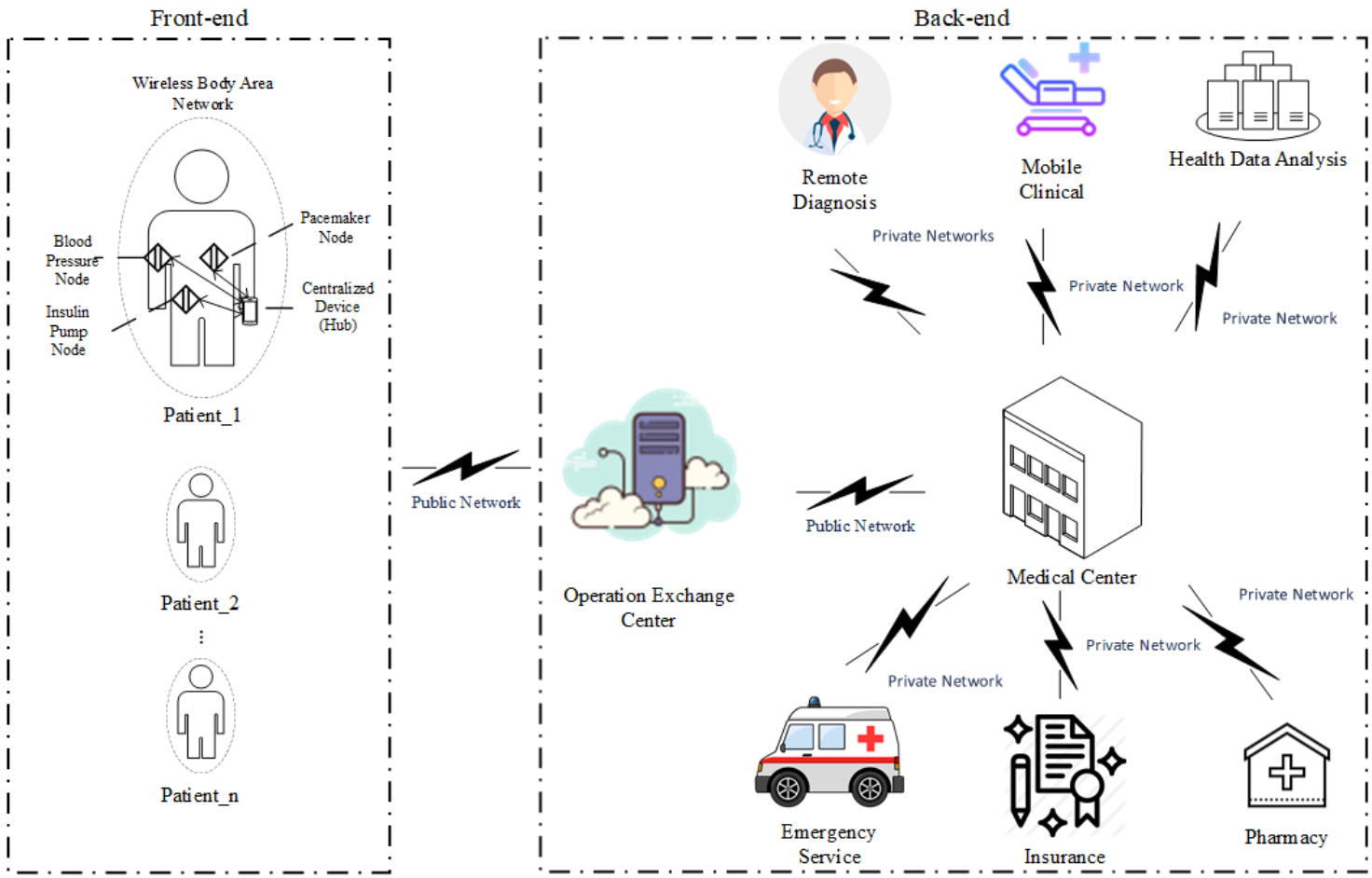



Figure 1–1: Architecture of an eHealthcare system

Table 1–1: Biomedical data types and its corresponding sensors

| Biomedical Data | Biomedical Sensors |
|---|---|
| Electrocardiography (ECG) | [84], [113], [61] |
| Electroencephalogram (EEG) | [84], [22], [15] |
| Heart Rate | [43], [121], [34] |
| Glucose Level | [95], [94], [90] |
| Body Temperature | [98], [16], [93] |
| Blood Pressure | [96], [92], [91] |

Meanwhile, increasing types of biomedical data can be collected from patients and transmitted for further data processing and storage. This capability is enabled by the rapid advances in biomedical sensors as illustrated in Table 1–1, as well as wireless communication (such as the Fifth Generation of Cellular Mobile communication (5G) and Bluetooth Low Energy (BLE)).

However, there are two potential issues that still restrict the development of the eHealthcare system [65] [60]. First, the sensors on humans are extremely power-sensitive, especially the implanted sensors with limited power supply and inconvenience of battery change. The most commonly utilized wireless communication protocols in the proposed sensors are Bluetooth and Zigbee which are not dedicated and optimized for biomedical data transmission. Second, even though multiple methods have been proposed to ensure the privacy of confidential personal information [33] [33], there is no mature security protection mechanism established for the data in the eHealthcare systems [60].

Therefore, it is of great significance to investigate solutions for a complete, efficient, and reliable eHealthcare system.

## 1.2 Introduction to WBANs

In recent years, the concept of WBANs has attracted huge academic and industrial research attention since WBAN is a wireless communication protocol that is dedicated to biomedical data transmission in the circumstances of medical applications. As one of the most fundamental elements of the eHealthcare system, WBAN establishes the communication between the biomedical sensors attached or implemented in the human body and the centralized devices such as the smartphones or tablets as illustrated in Figure 1–2.

There are multiple advantages that WBANs could provide. First, WBAN is the first wireless communication protocol which is dedicated to wireless data transmission between biomedical sensors and centralized devices. The network unifies the communication methods among the biomedical sensors, and between the sensors and centralized devices. Second, multiple methods of optimization can be applied, based on the characteristic of biomedical data collected, instead of obeying a wireless protocol such as Bluetooth or Zigbee which are not tuned for the communication of remote healthcare devices [65]. Third, WBANs address the interference issue caused by various communication protocols around the surface of the human body.

In 2012, the IEEE 802.15.6 standard for WBANs was released, which specifies and regulates the detailed specifications in the network, such as the security requirements, baseband processing procedures, frequency, and channels [51].

Based on the specifications of the IEEE 802.15.6 standard, evaluation of performance between WBANs and other widely utilized wireless communication technologies such as Bluetooth, Zigbee, and WIFI in various perspectives has been performed

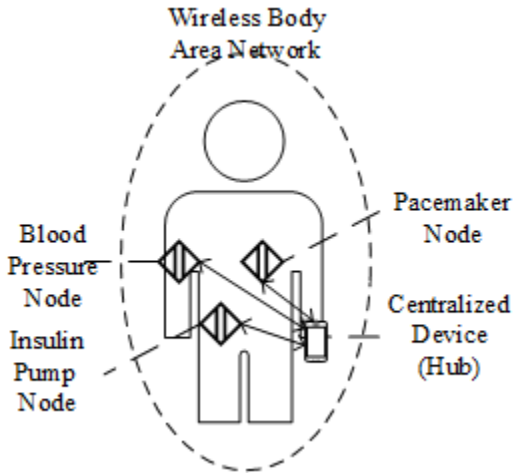



Figure 1–2: Architecture of a typical WBAN

to analyze the potential advantages WBANs can provide in biomedical data transmission. According to the simulation results of the evaluation, WBANs illustrate the advantages in power consumption, privacy protection, and efficient communication for biomedical data [65].

For instance, the power consumption of WBAN systems is between approximately 0.1 mW to 5 mW when the transmitting data rate is 1 Mbps, while for the same transmitting data rate, Bluetooth consumes between approximately 5 mW to 100 mW power. In this case, a typical AAA battery can last approximately 1 year for WBAN systems, while it can only last less than a month for Bluetooth systems [65] as illustrated in Table 1–2.

In terms of the security specifications, there are specific requirements in WBANs security processes. As mandated by the IEEE standard 802.15.6, three security levels, Level 0, Level 1, and Level 2, have been specified to classify the communication process in WBANs as demonstrated in Table 1–3 [51]. The security level of a specific

Table 1–2: Comparison among different wireless communication technologies [65]

| Wireless Communication Technology | Power Consumption (mW) | Battery Life | Typical Range (meters) |
|---|---|---|---|
| Bluetooth | 5 to 100 | 1 day to 4 weeks | 100 |
| Zigbee | 5 to 60 | 3 days to 5 weeks | 10-20 |
| Z-Wave | 2 to 40 | 1 week to 2 months | 100 |
| WBANs | 0.1 to 5 | 6 weeks to 12 months | 3 |

Table 1–3: Security levels of communication in WBANs

| Security level | Security Method | Typical information contained |
|---|---|---|
| 0 | None | Time stamp |
| 1 | Authentication | Name, age, gender, locations |
| 2 | Authentication and Encryption | Data collected from the biomedical sensors |

communication is determined by data type and privacy level. To be precise, for the lowest security level, Level 0, no algorithm or mechanism is applied during the data exchanging, and the channel is unsecured. In the case of Level 1, authentication is required during the communication, which provides a medium level of security in data exchanging. For the communication specified as security Level 2, they need to have both authentication and encryption (such as Elliptic Curve Cryptography (ECC)), which provides the highest protection during the data exchanging in WBANs.

Due to the advantages that WBANs provide, they have great potential in both medical and non-medical applications. Actually, multiple published papers have discussed the potential applications of WBANs into specific areas [7]. Concretely, [86] discussed the possibility to prepare the necessary medical treatments in advance when receiving the vital information regarding heart rate and irregularities of the heart captured by the sensors remotely cooperating with WBANs. Meanwhile, an

intelligent device for determining the time points for injecting insulin based on the glucose level monitored by the sensors has been proposed in [115]. Furthermore, [2] proposed that the sensors which could detect the allergic agents in the air could alert the patients and corresponding medical professional in advance.

However, there are some main facts restricting the development of WBANs. System on a Chip (SoC) is a commonly used platform for designing and implementing wireless communication protocols since it can achieve higher operation frequency and stability with lower power consumption compared to software-based solutions. However, unlike Bluetooth or Zigbee, there is no existing SoC solution for WBANs protocol, since it lacks mature Application-Specific Integrated Circuit (ASIC) based PHY, and security scheme for establishing the completed SoC architecture for WBANs. Meanwhile, the cooperation between the WBAN systems and existing medical data management system is relatively challenging. Finally, even though various designs and implementations of sensors and systems have been proposed by different researchers [103], while there is no unified and fair comparison platform for evaluating the performance in the identical environment for WBANs.

### 1.3 Objectives of the research

The general objective of the dissertation is to facilitate the emergence of eHealthcare systems with the low power and high-security WBAN systems performing on the patients' side and a trusted health data transmission and storage system running in the back-end as illustrated in Figure 1–1. The low power WBANs protocol could support the biomedical data transmission between nodes and hubs with ultra-low power consumption and proper security protection.

Even though the IEEE 802.15.6 WBANs standard was released in 2012, there are still multiple critical issues that we need to resolve for the wider acceptance of WBANs.

Initially, the real devices completely fulfilling the requirements of the standard are badly needed to help the spread of the WBANs technology and verify the standard.

Furthermore, since WBANs are transmitting extremely private biomedical data which is directly related to the health condition of the patients, WBANs technology will not be adopted if there are still security concerns regarding the WBANs. In other words, mature security schemes that not only meet the requirements of WBANs (hardware-efficiency and low power) but also can be resilient to common attacks such as timing attacks and simple power analysis, are required to ensure the secured communication in WBANs.

Last but not least, the interoperability and automation between the WBANs and other medical services including medical professional, pharmacies, insurance companies, and emergency systems are relatively challenging for conventional medical systems.

In future, blockchain technology could be a solution for the urgent need of trust, security, and privacy for the healthcare system. We would like to tune the blockchain to share data and provide smart contracts for healthcare systems, especially interoperating with WBAN systems. There are multiple potential use cases of the blockchain-based medical data systems. Among the most significant cases are Electronic Health Records (EHRs) for personalized medicine. In personalized

medicine, numerous sensors track various physiological state variables, such as blood sample data, exercise, nutrition, and various medicaments, and the collected data is used to infer the medicament dosing. The blockchain-based medical data system can resolve the challenges of providing the trusted prescriptions, medicaments, and sensor data in the exchange among medical practitioners, pharmacies, insurance companies and patients, such that no faulty data hinders the health/wellness regimen.

The demonstration of the objectives in the dissertation is done in a bottom-up manner. The specific objectives are described as follows.

First, based on the requirements of the IEEE 802.15.6 standard, Physical Layer (PHY) and the security scheme of WBANs will be designed and implemented.

Second, various optimization of the PHY and security scheme will be performed, and performance comparison between proposed designs and other published designs will be illustrated.

Third, an eHealthcare system which can not only meet the requirements of the security scheme and PHY of WBANs but also can interoperate with WBANs will be investigated.

Finally, an evaluation of all proposed modules will be illustrated to demonstrate that the performed designs are functional.

## 1.4 Contributions of the dissertation

The goal of WBANs is to establish a low power, high security, and stable real-time eHealthcare system which contains the WBAN systems in the front-end, and data exchange and storage system in the back-end. In terms of the general contributions, this dissertation proposes ASIC solutions for the front-end which completely

meets the requirements of PHY and security scheme in the IEEE 802.15.6 WBANs standard for the first time and a blockchain-based data exchange and storage system for WBANs has been proposed for the back-end. In addition, to evaluate various designs in WBANs, the dissertation also proposed a unified evaluation platform for WBAN systems. In summary, we make a required step for the development of WBANs, especially for the low power ASIC designs for WBANs protocol, and the blockchain-based data exchange and storage system for WBANs provides a feasible solution for trusted medical data management for modern medical institutions.

The detailed contributions of this dissertation are illustrated as follows:

A) For addressing the fundamental communication issues of WBANs, a baseband processing ASIC for WBAN systems is proposed, which supports all the methods of modulation and frequency channels specified in the IEEE 802.15.6 standard for the first time. Moreover, for optimizing the power consumption of the baseband processing ASIC, a *stochastic computing-based* Bose–Chaudhuri–Hocquenghem (BCH) decoder for WBAN systems with lower system complexity is developed.

B) In order resolve the security concerns of WBANs, a security scheme for WBANs is proposed based on the security requirements of WBANs. Furthermore, to optimize the performance of the proposed security scheme for WBANs, an encryption method that utilizes the characteristic values of the body channel is added. In addition, the proposed security scheme for WBANs is designed as ASIC for the first time to achieve the ultra-low power consumption requirement of WBANs.

C) To guarantee that the biomedical data transmitted among WBAN systems and other components in the eHealthcare system is trusted, a blockchain-based

eHealthcare system interoperating with WBAN systems is designed. Benefitting from the combination of WBANs and blockchain technology, the proposed eHealthcare system achieves low power, low hardware cost, and stable communication in the WBANs front-end, while the immutability and non-repudiation properties of the blockchain back-end offer powerful anti-tampering logging and auditing in the back-end.

D) A Software Defined Radio (SDR) based evaluation platform for WBAN systems is developed to provide a unified evaluation environment for the fair comparison among various designs and implementations for WBAN systems. All components supported by the IEEE 802.15.6 standard are built in the platform and available for establishing a standard communication link in WBANs. Meanwhile, every individual component can also be replaced or modified by other designs to evaluate the performance in the communication link of one or multiple certain blocks in WBAN systems.

## 1.5 Contributions of authors

There is a list of publications illustrated all the articles written by the author on page 161. The dissertation contains 3 published journal papers (#1, #2, #3), 2 conference papers (#9, #10), and 1 journal manuscript under review (#4). I would like to declare that I am the first and principal author among the co-authors. In general, my contributions to the articles including conducting the research studies, collecting and preparing the data, proposing the models, analyzing the data, implementing the designs, and writing the manuscripts. Concretely, in terms of my contributions

in article #3, after analyzing the network requirements, I proposed the system architecture of the baseband processing module, simulated the design with software, implemented the design by hardware language, verified and evaluated the baseband processing module in FPGA. In the articles #2, #9, and #10, I was responsible for proposing the system architecture of the security scheme for WBANs, proposing the mechanisms of authentication and encryption, implementing the design by hardware language, evaluating the design in FPGA, and analyzing the security characteristic under side channel attacks. I brought up the idea of the blockchain based eHealthcare system interoperating with WBANs initially in article #4. The hardware implementations of WBANs parts, the structure of the blocks and transactions in the eHealthcare system, and the Hyperledger implementation were also done by me. In the article #1, to address the demand for evaluating different designs for WBAN systems in a unified testing environment, I proposed and implemented a unified evaluation platform in an FPGA for WBAN systems. The author's supervisor, Prof. Zeljko Zilic provided guidance, comments, editorial revisions, and research funding throughout the entire process. Kaining Han contributed to the concept of stochastic computing, and part of the software simulation in the articles #2, #3, and #9. In article #4, Anastasios Alexandridis helped to implement the proposed work of the blockchain part in the Hypterledger. Zhiyu Chen did the verification of the evaluation platform for WBAN systems in the circumstances of narrowband communication in the article #1. Yu Pang and Jinzhao Lin are responsible for the post-synthesis and fabrication of the ASICs. The other co-authors contributed by helping in providing comments, and editing the papers.

## 1.6 Organization of the dissertation

The remainder of this dissertation is structured as follows. Chapter 2 presents the background of WBANs and the general specifications and requirements of the IEEE 802.15.6 standard. Afterwards, a baseband processing ASIC for narrowband communication in WBANs is proposed in the Chapter 3, and the optimized stochastic computing based BCH decoder for WBANs is also discussed in the chapter. Moreover, Chapter 4 illustrates the proposed security scheme and corresponding ASIC implementation for WBANs. Meanwhile, to further increase the security performance and decrease the system complexity of the security scheme, an encryption method by using the characteristic value of the body channel for WBANs is discussed in this chapter. Furthermore, Chapter 5 presents a blockchain-based eHealthcare system interoperating with WBAN systems, which provides a trusted data transmission and storage system benefiting from the blockchain technology. In Chapter 6, to provide a fair and unified evaluation environment for various WBANs designs, an SDR based evaluation platform for WBAN systems is illustrated. Last but not least, Chapter 7 concludes the performed work and discusses the potential work for the future.

# CHAPTER 2
# Wireless Body Area Network Background

This chapter reviews the background of WBANs including the development history of WBANs, the structure of WBANs, Radio Frequency (RF) characteristic of WBANs, general requirements of WBANs, and constraints of WBANs.

## 2.1 History of WBANs

WBAN is a subset of Wireless Personal Area Networks (WPANs) whose goal is to provide data transmission protocol among different personal electronic devices such as computers, smartphones, tablets, and personal digital assistants in short range between few center meters to few meters. The early development of WPANs was first made at Massachusetts Institute of Technology (MIT) in the 1990s where the initial purpose was to establish the communication among different information devices and use the electric field sensing to determine the position of human beings [65]. Based on the requirements of WPANs, various wireless network technologies such as Bluetooth and Zigbee have been proposed and made great success in the commercial market.

However, the limitations of WPANs in medical situations caused by close proximity to the human body tissue requires a novel communication standard. For the wireless communication in medical circumstances around/in the human body, the

novel standard should not only overcome the limitations of WPANs, but also provide an efficient, low power, and reliable network while transmitting biomedical data in medical applications.

To address such a demand, the IEEE 802.15.6 working group was established working on the standard of WBANs. In April 2010, the working group made the first draft of the communication standard of WBANs which optimized for lower power on-body/in-body nodes for medical and non-medical applications [65]. The official version was approved and released publicly in February 2012.

The goal of the IEEE 802.15.6 is described as follows: *To develop a communication standard for low power devices and operation on, in or around human body (but not limited to humans) to serve a variety of applications including medical, consumer electronics, personal entertainment, and other.*[42] A demonstration of the high-level structure is shown in Figure 2–1.

## 2.2 Structure of WBANs in IEEE 802.15.6

The IEEE 802.15.6 standard specifies three types of communication: Narrowband (NB), Ultrawide-band (UWB), and Human Body Communication (HBC). Each communication type defines various configurations for the network. However, the processing flow is similar for different communication in WBANs. As specified in the IEEE 802.15.6 WBANs standard [42], the transmission flow of WBANs is mainly separated into four parts which are Medium Access Control (MAC) layer, security scheme, PHY, and the RF front end, as shown in Figure 2–2. Initially, the MAC layer specifies the MAC frame format and the communication modes in the network [89], which requires a microcontroller unit (MCU) to process. Afterwards, the security

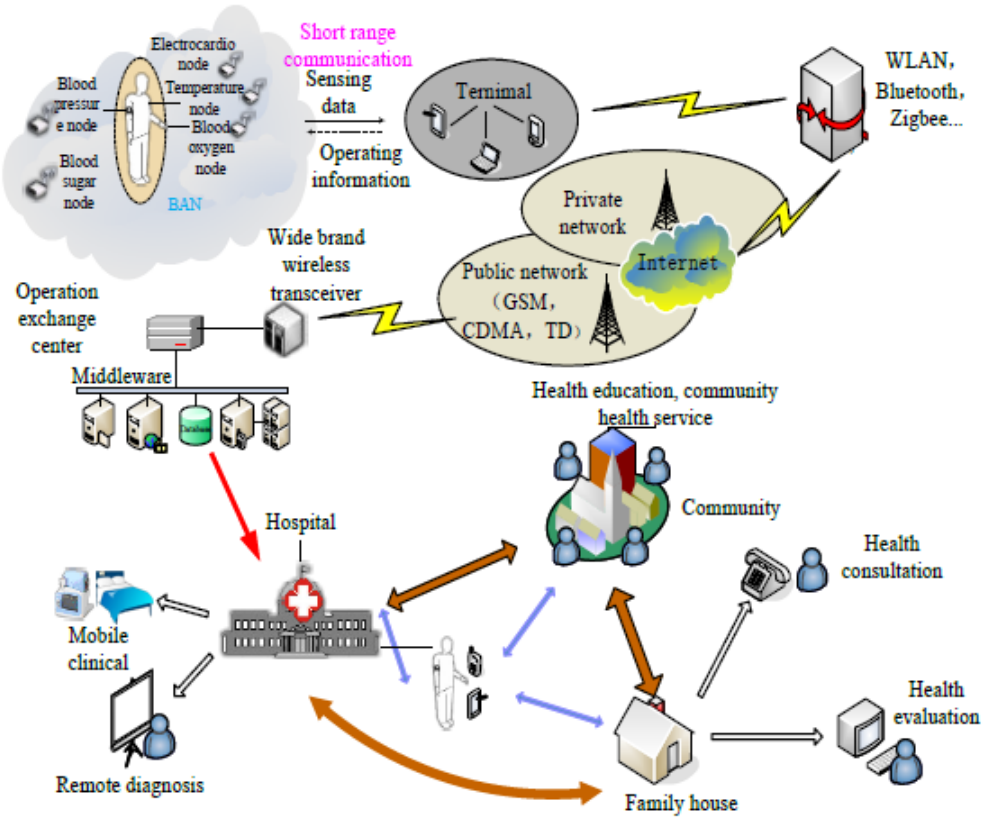



Figure 2–1: Structure of WBANs application circumstances

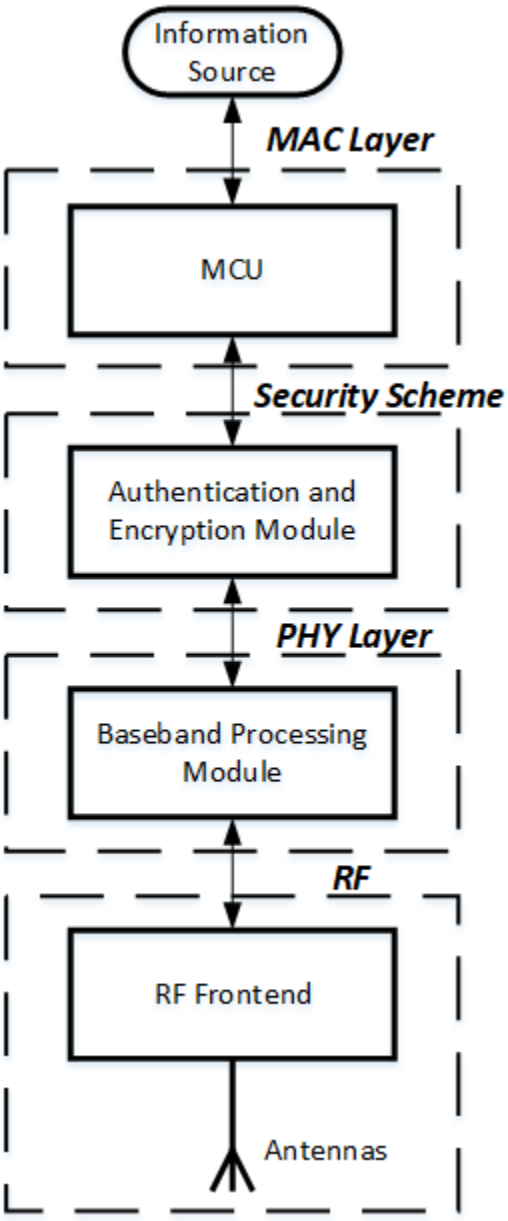



Figure 2–2: Transmission flow of WBANs that has been specified in the IEEE 802.15.6 standard

scheme needs to determine whether a specific communication needs to be authenticated and encrypted, based on the security level of the communication. The PHY involves the baseband processing module, where it processes the original binary data from the security scheme, into a format that is suitable for processing in the RF front end, where it is physically transmitted. Precisely, the responsibility of the baseband processing module is the activation and deactivation of the radio transceiver, clear communication assessment, and data reception and transmission [89]. Last but not least, the RF front end converts the digital data into an analog signal modulated at the right frequency, passes the modulated signal to an amplifier, and transmits it by the antenna (vice versa for the receiver).

### 2.2.1 MAC layer of WBANs

Placed above the PHY, the MAC layer of IEEE 802.15.6 is designed to control communication access. To do this, the MAC layer divides the entire communication into a chain of superframes through the hub (coordinator). At the boundary of these superframes, the hub chooses beacon periods of equal length to bound each superframe. If needed, one could shift the offset of the beacon period through the hub. The superframes will be normally sent in each beacon period [65], unless there is a restriction by regulations in the Medical Implant Communication Service (MICS) band or the superframes are inactive.

Figure 2–3 provides an overview of the structure of superframes in the standard. The superframe can be divided into three different components, the MAC header, the MAC Frame Body, and the Frame Check Sequence (FCS). With a length of 7 Bytes, the MAC header can be further divided into Recipient ID, Sender ID, WBANs ID,

and Frame Control, which contains information such as protocol version, ack policy and so on. The MAC Frame Body has a variable length; it contains Low-Order Security Sequence Number, Frame Payload with selected types, and MIC. The last 2 bytes of a MAC frame is the FCS to detect possible errors in transmission. The standard specifies the CRC-16-CCITT sequence to be used in error detection. The CRC polynomial is shown in Equation 2.1, where $a_{15}$ is the LSB of the field, $a_0$ is the MSB, and $a_{15}$,$a_{14}$,...,$a_0$ are the binary coefficients.

$$G(x) = x^{16} + x^{12} + x^5 + 1 \tag{2.1}$$

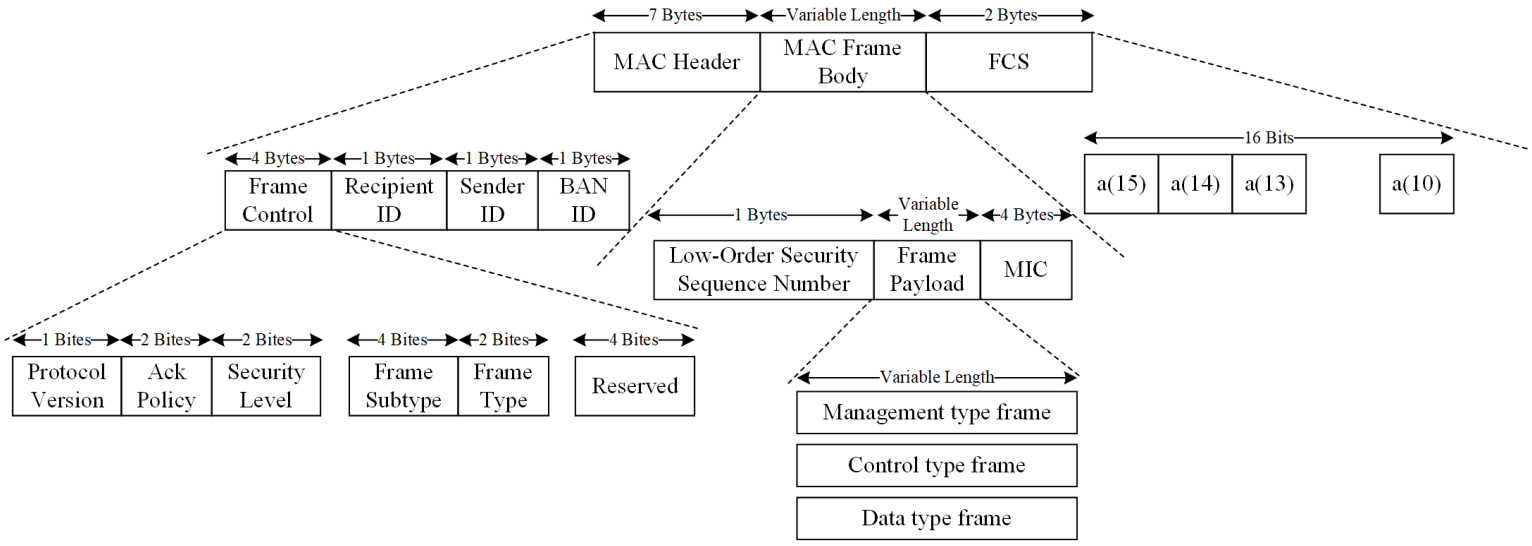



Figure 2–3: The frame structure of a general MAC frame defined in IEEE 802.15.6

### 2.2.2 PHY of WBANs

There are three main jobs that PHY of WBANs is responsible for. First, PHY needs to activate and deactivate of the radio transceiver based on the requirements of the upper level (MAC or security scheme) for power saving purpose. Second, the PHY shall do the clear channel assessment (CCA) which includes carrier sensing and energy detection for the current channel. Finally, the PHY is responsible for the data transmission and reception [65].

As mentioned before, there are three types of communication specified in the IEEE 802.15.6 standard, which are NB, UWB, and HBC. Each type of communication is corresponding to their specific PHY implementation since different types of communication has specific specifications in PHY. For instance, the frequency and bandwidth are different for each type of communication as illustrated in Table 2–1. In addition, other specifications such as modulation/demodulation, encoding/decoding methods, and communication technology are also different. Detailed specifications of each type of communication are illustrated in Chapter 3.

### 2.2.3 Security scheme of WBANs

The IEEE 802.15.6 standard specifies three security levels for all communication in WBANs, which is Level 0, Level 1, and Level 2, respectively. Level 0 is unsecured communication, where neither authentication nor encryption is required. Public information, such as time stamps, which is neither critical nor private, could be transmitted at this security level. Meanwhile, the communication of security Level 1 contains private, but not critical data, such as names, ages, and locations. This data is not significant for the physical conditions of the patients; however, they would

Table 2–1: Frequency and bandwidth for different communication in WBANs

| Types of Communication | Frequency (Hz) | Bandwidth (Hz) |
|---|---|---|
| NB | 402-405 M | 300 k |
| | 420-450 M | 300 k |
| | 863-870 M | 400 k |
| | 902-928 M | 500 k |
| | 950-958 M | 400 k |
| | 2.36-2.4 G | 1 M |
| | 2.4-2.4385 G | 1 M |
| UWB | 3.2-4.7 G | 499 M |
| | 6.2-10.3 G | 499 M |
| HBC | 16 G | 4 M |
| | 27 G | 4 M |

still not want to release it to the public. In these cases, authentication is required while encryption is not involved. In the case of the most critical data, such as blood pressure, heart rate, and parameters for a pacemaker, it is a requirement for them to be transmitted at Level 2. Both authentication and encryption are mandatory for Level 2 communication.

In terms of the methods implementing authentication and encryption, the standard specifies the certificate validation as the authentication method and ECC as the encryption method. Based on the specifications, multiple security schemes have been proposed to implement and even improve the security protection of WBAN systems. Concretely, lightweight data authentication schemes have been proposed in [27] and [80], which achieved much lower power consumption than conventional WBANs security schemes. Moreover, [116] and [72] proposed data authentication and encryption methods by utilizing the data collected from the sensors to generate

dynamic keys, which simplifies the system complexity of the security scheme while increasing the security level.

## 2.3 Radio frequency characteristic of WBANs

The IEEE 802.15.6 standard covers a series of operating frequency bands: 402 MHz to 405 MHz, 420 MHz to 450 MHz, 863 MHz to 870 MHz, 902 MHz to 928 MHz, 950 MHz to 958 MHz, 2360 MHz to 2400 MHz, and 2400 MHz to 2483.5 MHz. Each frequency band includes several sub-channels which are shown in Table 2–2, where $g_1(n_c)$ and $g_2(n_c)$ are mapping functions used in the 420 MHz to 450 MHz and 863 MHz to 870 MHz frequency bands, respectively.

$$g_1(n_c) = \begin{cases} n_c, & 0 \leq n_c \leq 1; \\ n_c + 6.875, & 2 \leq n_c \leq 1; \\ n_c + 13.40, & n_c = 5; \\ n_c + 35.025, & 6 \leq n_c \leq 7; \\ n_c + 40.925, & 8 \leq n_c \leq 9; \\ n_c + 47.250, & 10 \leq n_c \leq 11; \end{cases} \tag{2.2}$$

$$g_2(n_c) = \begin{cases} n_c, & 0 \leq n_c \leq 7; \\ n_c + 0.5, & n_c = 8; \\ n_c + 1, & 9 \leq n_c \leq 12; \\ n_c + 1.5, & n_c = 13; \end{cases} \tag{2.3}$$

Table 2–2: The central frequency and number of sub-channels in each frequency band

| Frequency Band (MHz) | Relationship between $f_c$ and $n_c$ | Number of channels |
|---|---|---|
| 402 to 405 | $f_c = 402.15 + 0.30 \times n_c$ (MHz),$n_c = 0, ..., 9$ | 10 |
| 420 to 450 | $f_c = 420.30 + 0.50 \times g_1(n_c)$ (MHz),$n_c = 0, ..., 11$ | 12 |
| 863 to 870 | $f_c = 863.20 + 0.40 \times g_2(n_c)$ (MHz),$n_c = 0, ..., 13$ | 14 |
| 902 to 928 | $f_c = 903.20 + 0.40 \times n_c$ (MHz),$n_c = 0, ..., 59$ | 60 |
| 950 to 958 | $f_c = 951.10 + 0.40 \times n_c$ (MHz),$n_c = 0, ..., 15$ | 16 |
| 2360 to 2400 | $f_c = 2361.00 + 1.00 \times n_c$ (MHz),$n_c = 0, ..., 38$ | 39 |
| 2400 to 2483.5 | $f_c = 2402.00 + 1.00 \times n_c$ (MHz),$n_c = 0, ..., 78$ | 79 |

Table 2–3: Data rate supported on each frequency band

| 402 to 405 MHz | 420 to 450 MHz | 863 to 870 MHz<br>902 to 928 MHz<br>950 to 958 Mhz | 2360 to 2400 MHz<br>2400 to 2483.5 MHz |
|---|---|---|---|
| Data rate (kbps) | | | |
| 75.9 | 75.9 | 101.2 | 121.4 |
| 151.8 | 151.8 | 202.4 | 242.9 |
| 303.6 | 187.5 | 404.8 | 485.7 |
| 455.4 | | 607.1 | 971.4 |

Based on the different bandwidth on these frequency bands and using the corresponding PHY parameter configuration, the data transmission rate is shown in Table 2–3.

### 2.4 Requirements of WBANs in IEEE 802.15.6

Based on the specifications of IEEE 802.15.6 and the application circumstances of WBANs, there are several basic requirements of WBANs as demonstrated following [65].

• All devices in WBANs shall be capable of transmitting at -10 dBm and the maximum radiated transmission power shall not be larger than 0 dBm.

• Since the components in WBANs are extremely power sensitive and they have limited power supply for the nodes, power saving mechanisms shall be utilized.

• The bit rate supported in WBANs is between 10 kb/s to 10 Mb/s.

• The connection time for each node in WBANs shall be less than 3 seconds.

• The maximum connection nodes of each WBANs shall be more than 256.

• On-body and in-body WBANs shall be capable of coexisting within the range.

• Proper security scheme shall be utilized based on the security level of the communication.

## 2.5 Constraints of WBANs

There are still several factors constraint the development of WBANs.

First of all, even though WBANs have illustrated great potential in different areas, while most of the researches have been published related to WBANs are from the specific sensors side instead of the network side. In other words, the establishing of the whole networks of WBANs needs more research attention.

Second, the IEEE 802.15.6 standard released in 2012 specifies the communication in WBANs, and few modules cooperating with WBANs have been proposed such as [59] and [21]. However, a mature architecture implemented in a proper platform of completed WBANs structure is needed for establishing the whole network.

Third, the nodes in WBANs have an extremely limited power supply and there are strict requirements for power consumption in IEEE 802.15.6 standard. However, the reliability and security protection of the communication in WBANs is also significant. Therefore, power optimization for different layers in WBAN systems shall be investigated.

Fourth, as a wireless communication protocol, IEEE 802.15.6 does not specify a higher-level data transmitting and storage system to cooperate with WBAN systems. However, in realistic, it is more convenient for the users to have a higher-level data transmitting and storage system to manage the behaviors of the WBAN systems, which needs more research attention to.

Last but not the least, the lack of unified evaluation platform for WBAN systems leads to the situation that it is difficult to have a real performance test in application circumstances for a specific module for WBAN systems. Furthermore, different evaluation environment for different designs could also cause unfair performance comparison between different designs for WBANs.

# CHAPTER 3
# Baseband Processing Techniques in WBAN Systems

The development in the field of advanced biomedical sensors has resulted in a large volume of data being collected and transmitted wirelessly. The IEEE 802.15.6 WBANs standard has specified a communication protocol for WBANs, however existing general-purpose communication protocols such as Bluetooth and Zigbee are more widely used due to multiple reasons. One of the critical issues is the lack of baseband processing hardware modules that implement the standard. In this Chapter, the author initially proposes a baseband transceiver for NB communication implemented in ASIC, which meets the 802.15.6-2012 standard requirements. Compared to other published designs, the proposed implementation exhibits better performance and cost parameters, while also offering a more complete standard implementation. Furthermore, benefiting from the advantages of low complexity of stochastic computing circuits, stochastic computing based BCH decoder for WBAN systems has been proposed, which decreases the power consumption of the transceiver for WBANs.

## 3.1 Related work of baseband processing techniques in WBAN systems

Among baseband processing schemes proposed, Liu et al. [59] proposed an ultra-low power baseband transceiver Integrated Circuit (IC) for WBANs, and fabricated it in 0.18-um Complementary Metal-Oxide-Semiconductor (CMOS) technology in 2011. The bit error rate and packet error rate were demonstrated for evaluation purposes. However, since it was proposed before the standard of IEEE 802.15.6 was

released, the processing method does not meet the requirements of the standard, even though it exhibits some advantages at certain points.

Chen et al. [21] proposed a low power and area-efficient baseband processor for WBANs transmitters, based on the IEEE 802.15.6 WBANs standard in 2013. The processor was designed to achieve the specifications of the NB PHY in the standard. Moreover, two major optimizations, employing canonical signed digit coded filter for Differential Phase Shift Keying (DPSK) modulator, and applying clock gating technology, were implemented to minimize the power consumption. The corresponding receiver, however, was not proposed in the paper.

In 2014, a hardware platform involved a baseband processing module was proposed by Liang et al. [55]. It was implemented by an FPGA, an RF IC, and a Digital-to-Analog chip and obeyed the specifications of NB physical layer of IEEE 802.15.6 WBANs standard. The performance of the proposed implementation, such as throughput, operation frequency, and power consumption were evaluated, and a comparison to Zigbee was demonstrated at the same time. However, similarly to [21], the corresponding receiver implementation was not considered in the paper.

Chougrani et al. [23] proposed a UWB digital baseband architecture using impulse radio for WBANs, in 2014. The proposed architecture combines coherent and non-coherent receivers. The evaluation performed in FPGA illustrated the advantages of low packet error rate and bit error rate.

In 2015, Mathew et al. [62] proposed a complete NB physical layer transceiver implemented in FPGA that consists of both baseband transmitter and receiver blocks. Moreover, software-defined radio was used to optimize performance.

As it can be seen, even though a few baseband processing modules have been proposed, most of the works are based on the evaluation of FPGA implementations, while, one of them was synthesized using 0.18-um CMOS technology, but it was not quite fit for the IEEE 802.15.6 WBANs standard. Therefore, an ASIC implementation of baseband architecture, which consists of both transmitter and receiver that obey the IEEE 802.15.6 WBANs standard is proposed in this dissertation. The design is synthesized and evaluated using the Semiconductor Manufacturing International Corporation (SMIC) 65nm CMOS technology. Details regarding the verification and evaluation of the proposed ASIC are demonstrated in Section3.4.

## 3.2 Structure of the data packet in WBANs

In the specification of IEEE 802.15.6 WBANs standard, there are three types of communication that could be utilized in WBANs: NB, UWB, and HBC respectively, with each of them having various advantages, and presenting different implementation challenges. This chapter focuses on the physical layer of the NB channel. The standard Protocol Data Unit (PPDU) for NB has been illustrated in Figure3–1. Every PPDU contains three main components: PHY Convergence Protocol (PLCP) preamble, the PLCP header, and the PHY Service Data Unit (PSDU).

### 3.2.1 PLCP preamble

As seen in Figure 3–1, the 90-bit PLCP preamble is the initial data package that needs to be sent for every PPDU, and the goal of it is to assist the receiver in data packet detection, timing synchronization, and carrier-offset recovery. It is a combination sequence which contains a 63-bit m-sequence, specified in the standard, followed by the sequence "101010101010110110110110110 1".

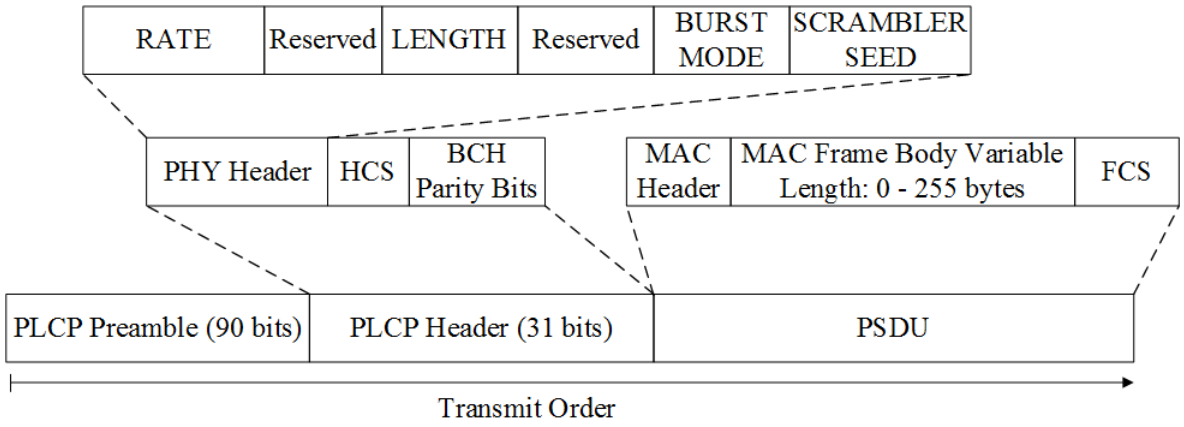



Figure 3–1: Standard PPDU structure

### 3.2.2 PLCP header

Following the PLCP preamble, a 31-bit PLCP header that contains a 15-bit PHY header, a 4-bit Header Check Sequence (HCS), and 12-bit BCH parity bits shall be sent. The purpose of the PLCP header is to provide the parameters related to the BCH encoder so that the receiver can decode the PSDU.

As the most significant part of the PLCP header, the PHY header is constructed by a 3-bit RATE, 8-bit LENGTH, 1-bit BURST MODE, and 1-bit SCRAMBLER SEED, while one bit is reserved, as illustrated in Figure 3–2. The encoding methods and corresponding meaning of them are specified in the standard.

According to the standard, the PHY header shall be protected with an HCS of Cyclic Redundancy Check 4 (CRC-4), while the HCS shall be the one's complement of the remainder, generated by the modulo-2 division of the PHY header by Equation 3.1.

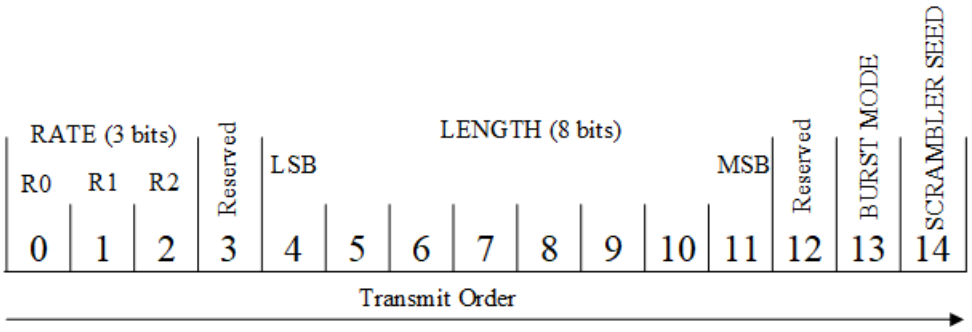



Figure 3–2: PHY header bit assignment

$$1 + X + X^4 \tag{3.1}$$

The BCH(n=31, k=19, t=2) code, which is a shortened code derived from the BCH(n=63, k=51, t=2) is utilized as the encoding mechanism of the PLCP header. The output of the BCH encoder is 12 bits together with the BCH parity bits.

### 3.2.3 PSDU

The PSDU is the most significant component of a standard PPDU packet since it contains the data from the MAC layer. More precisely, it consists of a 7-byte MAC header at the beginning of the sequence, a 2-byte FCS at the end of the sequence, and a 0-255 byte MAC frame body in the middle, containing the data.

## 3.3 Proposed baseband processing module for NB communication in WBANs

As it has been specified in the IEEE 802.15.6 WBANs standard, the baseband processing module for the transmitter in WBANs contains five blocks: BCH encoder, Spreader, Bitwise Interleaver, Scrambler, and Symbol Mapper. The receiver side needs to do the reverse process which consists of De-Symbol Mapper, De-Scrambler,

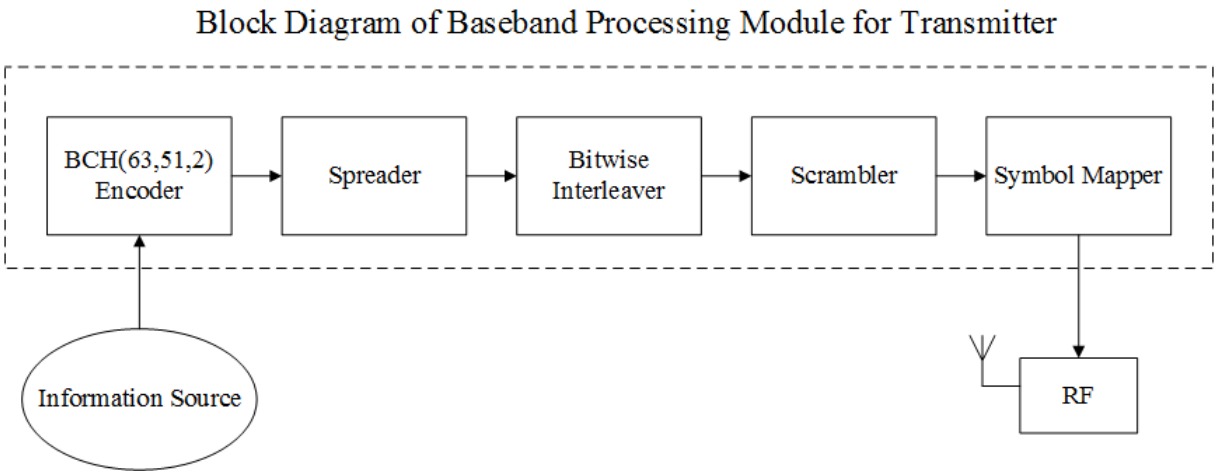



Figure 3–3: Block diagram of transmitter

Bitwise De-Interleaver, De-Spreader, and BCH decoder. The block diagrams of the transmitter end and corresponding receiver end are demonstrated in Figure 3–3 and Figure 3–4 respectively.

Both the PLCP header and PSDU follow the procedure illustrated in the baseband processing module block diagram, with slight differences in the BCH encoding (and decoding) step. The PLCP preamble is transmitted at the desired symbol rate and encoded using the same parameters as the PLCP header.

### 3.3.1 BCH encoder block

As mentioned, the PLCP header uses a systematic BCH code, where n=31, and k=19 to make the header more robust. This shortened BCH(n=63, k=51) code can be obtained by appending 32 shortened (zero) bits to the 19 information bits. For the PSDU, a systematic BCH(n=63, k=51) code is used. Appending shortened bits is performed to match the desired code rate, while the procedure is slightly different as the number of PSDU bits is vary.

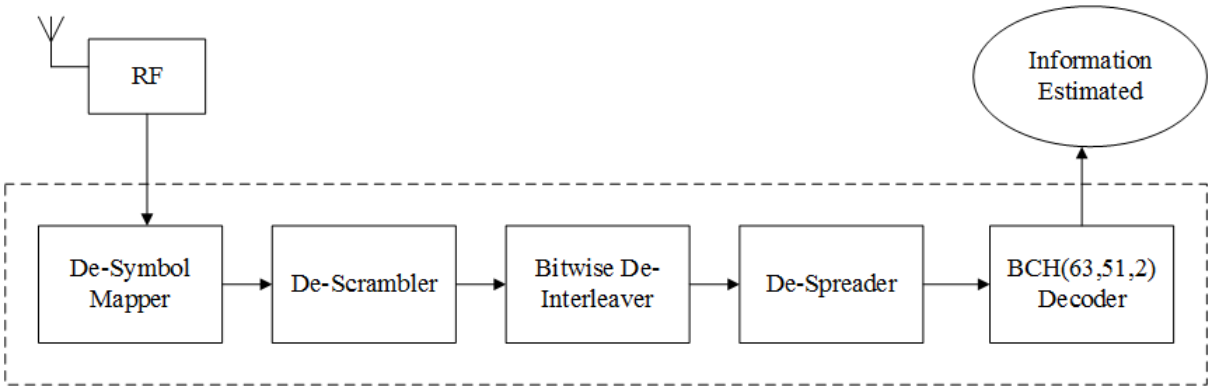



Figure 3–4: Block diagram of receiver

**Shortened bits**

First, the number of bits in the entire PSDU, $N_{psdu}$, is calculated by adding the number of bytes in the PSDU, then multiplying by 8 bits per byte, as shown in Equation 3.2.

$$\begin{aligned} N_{psdu} =& (Length_{MACheader} + Length_{MACframebody} \\ &+ Length_{MACframechecksequence}) * 8 \end{aligned} \tag{3.2}$$

Then, the number of codewords, $N_{cw}$, is calculated by taking the ceiling of the number of PSDU bits divided by the message bits ($k$), that is, the number is rounded up to the next integer after division, as shown in Equation 3.3.

$$N_{cw} = \left\lceil \frac{N_{psdu}}{k} \right\rceil \tag{3.3}$$

Here the difference between the PLCP header and PSDU encoding can be observed; for the header, the length is short, so the number of codewords is one, which means the computation is not necessary.

The number of shortened bits, $N_{short}$, is then calculated and padded to the $N_{psdu}$ bits prior to encoding. $N_{short}$ is calculated as shown in Equation 3.4.

$$N_{short} = (N_{cw} \times k) - N_{psdu} \tag{3.4}$$

The shortened bits are distributed equally over the $N_{cw}$ codewords. First, the parameter $N_{spcw}$ (shortened bits per codeword) is defined in Equation 3.5.

$$N_{spcw} = \left\lfloor \frac{N_{short}}{N_{cw}} \right\rfloor \tag{3.5}$$

Then, the first $(N_{short})mod(N_{cw})$ (mod indicating the remainder of integer division) codewords will be appended with $N_{spcw} + 1$ shortened bits, while the remaining codewords will be appended with $N_{spcw}$ shortened bits. In both cases of PLCP header and PSDU, the shortened bits are removed after the encoding process and are never transmitted.

**Parity bits**

The systematic BCH encoder will compute the parity bits for every codeword, as shown in Equation 3.6, where, the remainder polynomial $r(x)$ is defined as shown.

$$r(x) = \sum_{i=0}^{11} r_i x^i = x^{12}\ m(x)\ mod\ g(x) \tag{3.6}$$

where $g(x)$ is the generator polynomial $g(x) = 1 + x^3 + \cdots + x^{12}$ and $m(x)$ is the message polynomial $m(x) = \sum_{i=0}^{50} m_i \times x^i \; r_i$, where i=0 to 11, and $m_i$, where i=0 to 50, are elements of a 2 element Galois Field, GF(2).

Message and parity bits will be transmitted in order; $m_{50}$ and $r_{11}$ respectively will be the first ones transmitted, whereas $m_0$ and $r_0$ will be the last ones. As mentioned, the shortened bits will be removed before transmission.

**Padding bits**

Following the BCH encoding, padding bits are appended to the PSDU to align it for symbol mapping (modulation). The padding bits are zeros. The number of padding bits, $N_{pad}$, is a function of PSDU bits ($N_{psdu}$), codewords ($N_{cw}$), number of parity bits $(n-k)$, and modulation constellation size $M$, as shown in Equation 3.7.

$$\begin{aligned} N_{pad} = & log_2(M) \times \left\lceil \frac{N_{PSDU} + N_{CW} \times (n-k)}{log_2(M)} \right\rceil \\ & - [N_{PSDU} + N_{CW} \times (n-k)] \end{aligned} \tag{3.7}$$

where $N_{cw} = 0$ if the transmission is unencoded.

### 3.3.2 Spreader, bitwise interleaver, and multi-mode Symbol mapper blocks

**Spreader**

The spreader is a simple block that replicates input bits $S$ times on the output, where $S$ is defined to be a spreading factor. For $S = 1$, the output will be identical to the input. For $S > 1$ every bit will be output $S$ times before moving on to the next bit.

**Bitwise interleaver**

The bitwise interleaver is commonly used in digital communication systems to increase their robustness against errors. The interleaver operates on the output of the spreader and aims at lowering the effect of burst errors. By interleaving, an error that could affect several bits in a row will have corrupted random bits in the transmission after de-interleaving, uniformly distributing errors across the transmission. Consequently, less error correction is needed. The interleaving operation has been defined by the standard.

**Scrambler block**

The functionality of the scrambler is to avoid direct current bias in the data bit streams. The scrambler performs modulo-2 addition (XOR) between its input and x[n] to produce its output, where x[n] is defined as shown in Equation 3.8.

$$x[n] = x[n-2] \oplus x[n-12] \oplus x[n-13] \oplus x[n-14] \tag{3.8}$$

Figure 3–5 shows the block diagram of the scrambler. The minus sign is used to indicate a delay. This delay is equal to the time it takes to scramble one bit, that is, for the next bit all the values will have rotated around, and a new x[n] will be computed.

The Scrambler Seed (SS) is a 1-bit rolling counter. It can take two values: either 0 or 1. It rolls down to 0 when incrementing at 1. For each seed, there exists an initialization vector that defines all the delayed values x[n-D] at the moment operation begins.

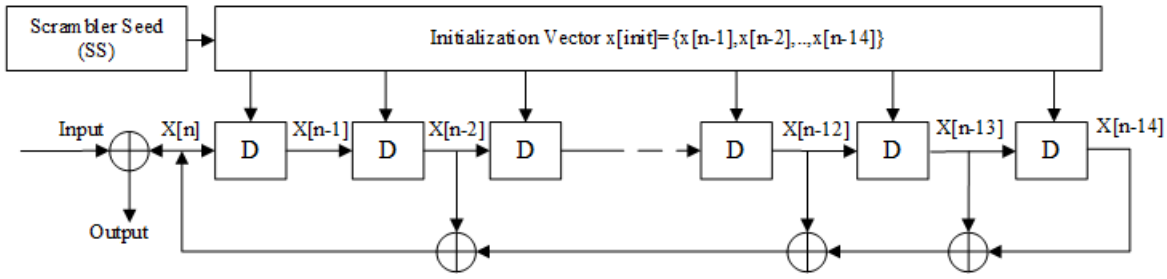



Figure 3–5: Block diagram of scrambler

The starting seed value is defined in the PLCP header, and it will increment for every frame sent. When a new frame is sent, the scrambler seed is updated, and a new initialization vector updates all the delayed values of x[n].

**Multi-mode symbol mapper**

As defined in the IEEE 802.15.6 WBANs standard, the PHY should support three modulation types to meet the requirements of different data transmission rate. In the proposed design, a flexible multi-mode symbol mapper has been proposed, which supports Differential Binary Phase Shift Keying (DBPSK), Differential Quadrature Phase Shift Keying (DQPSK), and Differential Eight Phase Shift Keying (D8PSK) modulation. Besides, the initial phase and constellation points are also flexible. To reduce the dynamic power consumption, the clock gating technology is also applied in the proposed design. At the receiving end, the corresponding symbol De-mapper is implemented.

## 3.4 Implementation and evaluation of the proposed baseband processing module for NB communication in WBANs

The performance of baseband processing of the proposed NB PHY for WBANs was evaluated in Matlab. Three modulation types, DBPSK, DQPSK, and D8PSK,

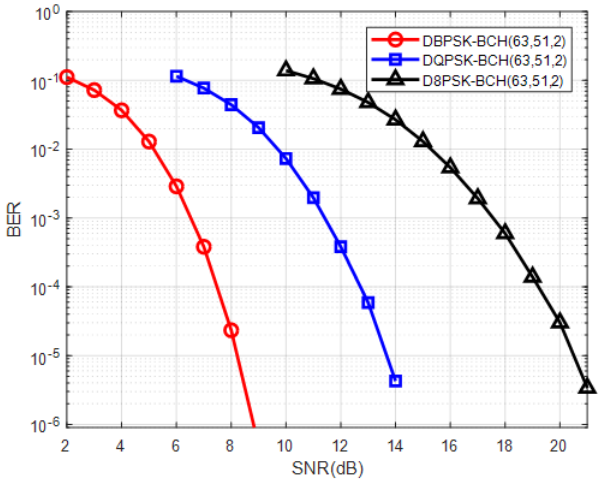



Figure 3–6: Simulation results of various modulations

which cover all the modulation methods specified by the IEEE 802.15.6 WBANs standard were evaluated. Meanwhile, an Additive White Gaussian Noise (AWGN) was added to simulate the transmission environment. The simulation results are illustrated in Figure 3–6, which demonstrates the relationship between Bit Error Rate (BER) and Signal-to-Noise Ratio (SNR) applied in various modulation methods[31].

In terms of hardware implementation, the proposed baseband processing module was implemented in VHDL. Then, it was synthesized by Synopsys using a density and performance optimized high speed library of the SMIC 65nm CMOS technology. Figure 3–7 and Table 3–1 illustrate the layout and synthesis results of the proposed design respectively.

Comparison of performance between the proposed design and previous publications has been given in Table 3–2, featuring process technology, power supply,

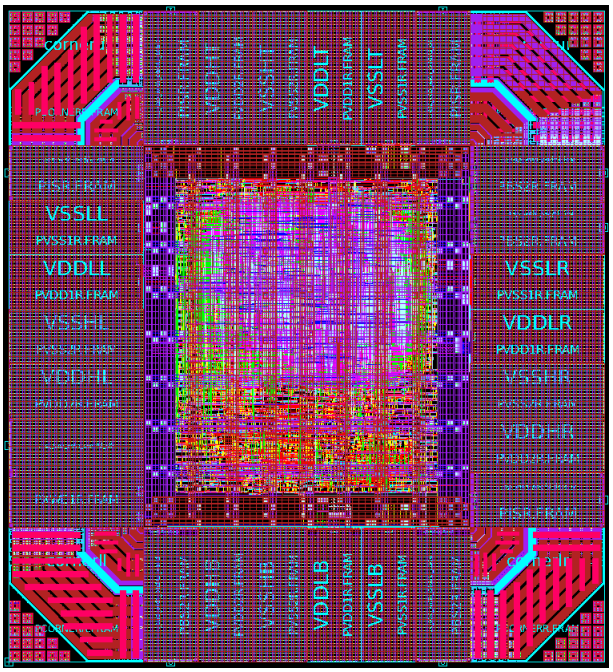



Figure 3–7: Layout of proposed design

Table 3–1: Final synthesis results of proposed ASIC

| Technology | SMIC 65nm CMOS technology |
|---|---|
| Die Area | 0.325 $mm^2$ |
| Core Area | 0.069 $mm^2$ |
| Maximum Frequency | 869.5 MHz |
| Operating Frequency | 10 MHz |
| Maximum Throughput | 10 Mbps |
| Power in Operating Frequency | 32.8 $\mu$W |
| Latency | 8 $\mu$s |

modulation method(s), power of transmitter and receiver, maximum throughput, operating frequency, core size, and energy consumption per bit ($E_b$).

As it can be seen in Table 3–2, the proposed design has the advantages of high throughput, low transmission power, high operation frequency, multiple modulation method support, and high energy efficiency, all while maintaining the relatively small area.

Table 3–2: Performance comparison between proposed design and other publications

| Publication | This Design | [59] | [21] |
|---|---|---|---|
| Process Technology(nm) | 65 | 180 | 130 |
| Power Supply (V) | 1.2 | 1.1 | 1.0 |
| Modulation | DBPSK, DQPSK, D8PSK | BFSK[a] | DBPSK, DQPSK, D8PSK |
| Core Power of Transmitter ($\mu$W) | 1.69 | 34 | 9.89 |
| Core Power of Receiver ($\mu$W) | 20.46 | 39.6 | Not Applicable |
| Maximum Throughput(Mbps) | 10 | 0.625 | 0.97 |
| Operating Frequency(MHz) | 10 | 4 | 1.2 |
| Core Size($mm^2$) | 0.069 | 0.31 | 0.016[b] |
| $E_b(pJ/bit)$ | 3.2 | 294.4 | 10.1 |

[a] BPSK is not supported in the IEEE 802.15.6 WBANs standard

[b] It only contains the transmitter without the receiver

## 3.5 High-performance BCH decoder for WBAN systems using stochastic computing

BCH codes have been accepted as the error correction coding scheme by the IEEE 802.15.6 standard for power and energy sensitive WBAN systems. Soft-decision BCH decoders are attractive for the reason that the decoding gains result in significant transmitting energy reduction. Stochastic computing is a promising low power and low hardware cost implementation candidate for BCH soft decision decoders. In this section, stochastic computing based soft decision decoder is presented for the BCH codes defined in the IEEE 802.15.6 standard. According to the evaluation results, the proposed design has the advantages of energy consumption and hardware cost while approaching the Maximum Likelihood (ML) decoding performance in terms of Block Error Rate (BLER). In addition, the proposed design requires no noise power estimation, further simplifying the WBANs receiver.

In 2012, the IEEE 802.15.6 standard [42] was released for the specifications of WBAN systems. According to this standard, to improve the reliability of the communication, the BCH code has been specified as the error correcting code scheme. Besides, benefiting from the coding gains of BCH codes, the transmitting power of the sensor end could be reduced, enhancing the usage duration of the energy and power sensitive sensors.

In terms of BCH decoding methods, the Hard-Decision Decoder (HDD) for BCH code is commonly used in WBANs due to the simple hardware implementation structure. However, in view of system power consumption, a Soft-Decision Decoder (SDD) is more attractive since the better BER performance leads to power reduction in the transmitting side. Based on the evaluation performed by [39], ML decoding provides

the best BER performance for SDD, while the huge complexity results in impractical hardware cost. Regarding the BCH SDD in WBANs, multiple architectures with acceptable hardware cost have been proposed [110],[45]. However, the BER performance gap between published decoders and the ML decoder is still relatively large.

As an implementation technique, stochastic computing can carry out complex computations with simple logic and has the advantages of low implementation complexity, short critical path, and high fault tolerance. Several stochastic computing based decoders have been proposed in prior literature for various codes such as such as Reed-Solomon codes [40] [53], LDPC codes [87],[66], Turbo codes[70], and Polar codes [111]. The advantages of lower hardware cost, shorter critical path, and higher throughput are observed for stochastic computing based decoders compared to conventional binary decoder designs.

For SDD of BCH codes, the core decoding is based on the hard-decision kernel. While the biggest challenge is the efficient search of the test pattern. In this section, a novel stochastic computing based BCH decoder is proposed, where the test pattern is generated with a stochastic method.

The detailed evaluation and analysis results, such as performance and latency evaluation of BCH codes for $\frac{\pi}{4}$-DQPSK modulated WBAN system, are presented in this section. The novelty and contributions of this design can be summarized as

- A novel stochastic computing based test pattern generation method is proposed to achieve efficient search of good test pattern candidate, which contributes to the approaching ML decoding performance.

- The combinational logic based hard-decision decoding kernel is designed to save memory consumption and total hardware cost.
- CRC aided early stopping criteria and Noise-Dependent Scaling (NDS) are utilized to reduce the decoding latency and enhance the throughput and eliminate the noise power estimation module.
- to apply the proposed design to a practical WBAN system defined as IEEE 802.15.6 standard, soft-decision demodulation for $\frac{\pi}{4}$-DQPSK is adopted in the proposed design to generate the log-likelihood ratio (LLR) as the soft-input of the stochastic BCH decoder.

### 3.5.1 Background of BCH code and stochastic computing

In this subsection, the basis of BCH code and stochastic computing are introduced.

**BCH codes**

A binary BCH code with code length $N = 2^m - 1$ is designed based on the Galois field GF($2^m$), where the information length $K \geqslant N - mt$ is selected according to the required error correcting capacity $t$. In the IEEE 802.15.6 standard, the $(N = 63, K = 51, t = 2)$ BCH code is designed over GF($2^6$), which encodes the information bits $u_1^K = \{u_1, u_2, ..., u_K\}$ to codeword bits $x_1^N = \{x_1, x_2, ..., x_N\}$.

The commonly used HDD algorithm for BCH is Berlekamp-Massey [105]. However, once the error correcting capacity $t$ is low such as the BCH code specified in IEEE 802.15.6, where $t = 2$, the Look-up-Table (LUT) [67] and Peterson Rule-based [109] HDD are more suitable [110]. Benefiting from the efficient architecture of HDD

kernel, the HDD based SDD, such as the type-II Chase-based SDD [58], shows advantages for hardware compared to the Maximum Likelihood (ML) decoding [97] and Generalized Minimum Distance (GMD) [32].

**Soft-Decision decoding of BCH codes**

Type-II Chase-based decoding algorithm is an efficient SDD for BCH codes. The decoding steps could be summarized as,

(1) Determine the searching radius $r = \lfloor d_{min}/2 \rfloor$, where $d_{min}$ is the minimum Hamming distance of the BCH code.

(2) Traverse the $r$ least reliable bits to generate the $2^r$ test patterns.

(3) Decode each of the test patterns using the HDD kernel and mark the successfully decoded test pattern as a candidate.

(4) Calculate the Euclidean distance for all of the decoding result candidates and output the optimal candidate with the smallest Euclidean distance as the final decoding result.

Even though some optimization methods are proposed to reduce the number of redundant test patterns, such as the two-stage method in [20], the searching of least reliable bits still involves huge complexity.

**Stochastic computing**

In stochastic computing, a number is represented with a random bit stream by comparing it with a uniformly distributed random number $R(t) \sim U(0, 1)$. Using a stochastic representation can map complex arithmetic functions to simple bitwise logical operation. For example, multiplication, which has high hardware cost in the conventional binary system, is mapped to a single AND gate in stochastic computing.

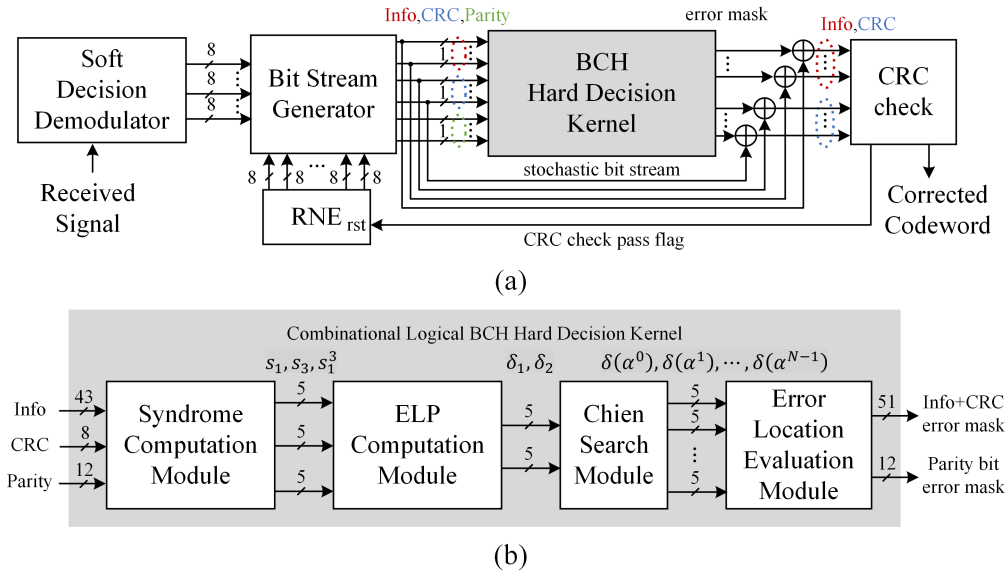



Figure 3–8: The hardware architecture of the proposed stochastic BCH decoder: (a) Top level architecture; (b) BCH HDD kernel architecture.

In this section, stochastic computing has been utilized to represent and randomize the decoder soft input, while the decoding is processed in GF($2^m$) with binary logic.

### 3.5.2 Stochastic BCH decoder

The proposed stochastic BCH decoder consists of Bit stream generator, HDD kernel, and CRC check module, illustrated in Figure 3–8. The bit-stream generator produces test patterns to be used in a Chase-like scheme based on a HDD kernel [40][53].

**Stochastic bit stream generation**

The first step of the proposed stochastic BCH decoder is to transform the input log-likelihood ratios $LLR_n$ to probabilities $P_n \triangleq P(y_n|x_n = 1)$ and then represent

them with bit stream: $\{Y_n^{(t)} | Pr(Y_n^{(t)} = 1) = P_n\}$, where $n = 1, 2, ..., N$.

$$LLR_n = \log\left(\frac{P\left(y_n \mid x_n = 0\right)}{P\left(y_n \mid x_n = 1\right)}\right) \tag{3.9}$$

$$P\left(y_n \mid x_n = 1\right) = \frac{1}{1 + \exp\left(LLR_n\right)} \tag{3.10}$$

$$Y_n^{(t)} = \begin{cases} 1, & P\left(y_n \mid x_n = 1\right) \geq R(t); \\ 0, & otherwise; \end{cases} \tag{3.11}$$

The bit stream generator based on (3.9), (3.10) and (3.11) involves a large number of exponential operations, resulting in large hardware cost. The direct LLR-to-Stochastic (L2S) method [38] is applied to remove the exponential operations.

$$P\left(y_n \mid x_n = 1\right) \geq R(t) \Rightarrow LLR_n \leq ln\left[\frac{1}{R\left(t\right)} - 1\right] \tag{3.12}$$

$$Y_n^{(t)} = \begin{cases} 1, & LLR_n \leq R^{'}\left(t\right); \\ 0, & otherwise, \end{cases} \tag{3.13}$$

where $R^{'}\left(t\right) \triangleq ln\left[1/R\left(t\right) - 1\right]$ can be calculated with the uniformly distributed random number $R\left(t\right)$. The random number sharing scheme is also applied in this work to reduce the amount of Random Number Engines (RNE) [38]. Even though the bit stream generator adds slight hardware overhead, the proposed stochastic BCH decoder still illustrates lower hardware cost compared to conventional binary based BCH SDD since it does not contain the multiple bits represented test syndrome calculation module and sorting module.

The reason that the proposed stochastic BCH decoder can approximate to the performance of ML decoder is that the bit stream representation of the input LLRs can be considered as random searching, while the combination of the bit stream: $Y_{1\sim N}^{(t)}$ could be any codeword of the BCH codeword space. Therefore, with enough bit stream length, the whole codeword space can be covered by the random searching.

**Combinational logic based HDD kernel**

In HDD kernel, the first step is to compute the syndrome based on vector-formated bit stream $\mathbf{y} = [Y_1^{(t)}, Y_2^{(t)}, ..., Y_N^{(t)}]$ and parity check matrix $\mathbf{H}$ as,

$$\mathbf{s} = \mathbf{y} \cdot \mathbf{H}^T = [s_1, s_3], \tag{3.14}$$

where $\mathbf{s}$ is the syndrome vector. The second step is calculating the Error Location Polynomial (ELP). For the BCH code when $t = 2$ in WBANs, the ELP can be calculated as,

$$\delta(x) = 1 + \delta_1 x + \delta_2 x^2, \tag{3.15}$$

where $\delta_1 = s_1$ and $\delta_2 = (s_1^3 + s_3)/s_1$. The third step is to utilize Chien search module to allocate the error bits. All the possible values of $x = \alpha^i$ are tried in (3.15) to check whether it holds, where $i = 0, 1, ..., n-1$ and $\alpha$ is the primitive element of GF($2^m$). If $\delta(\alpha^i) = 0$, the $(n-i)$-th bit of the error mask vector is 1.

In the proposed design, the second and third step can be implemented with a LUT, which could shorten the critical path and increase the clock frequency. Benefiting from the combinational logic based syndrome module and LUT based ELP computation module and Chien search module, each bit in the input bit stream can be processed in one clock cycle, which contributes to higher throughput.

**CRC aided early stopping criteria**

To improve the decoding performance and reduce the decoding latency, CRC aided early stopping criteria is applied in the proposed stochastic BCH decoder. Based on the simulation results, the trade-off between the CRC error detection capability and effective Signal to Noise Power Ratio (SNR) loss is evaluated. Despite the increment in code rate and loss in effective SNR, the better coding gain is observed by using the CRC check. Therefore, the 8 bit CRC is applied in the proposed design.

### 3.5.3 Stochastic computing based WBANs receiver

In this section, the soft-decision demodulation for $\frac{\pi}{4}$-DQPSK and noise-dependent scaling method are presented.

**Soft-Decision DQPSK demodulation**

For the $\frac{\pi}{4}$-DQPSK specified in IEEE 802.15.6, every two information bits are mapped to a phase transformation, ["00","01","10","11"] is mapped to $\Delta\text{Phase} = [\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}]$. Thus, there would be $M = 8$ constellation points $\{C_m\} = \{e^{j\frac{m\cdot\pi}{4}}\}$, where $m = 0, 1, ..., M-1$.

The first step is calculating the phase transformation probability $\Pr(\Delta\text{Phase} = \frac{i\pi}{4})$ as,

$$P_t(\frac{i\pi}{4}) = \sum_{m=0}^{M-1} e^{\frac{[y_{t-1}-e^{j\frac{m\pi}{4}}]^2}{-N_0}} \cdot e^{\frac{[y_t-e^{j\frac{(m+i)\pi}{4}}]^2}{-N_0}}, \tag{3.16}$$

where $i = 1, 3, 5, 7$ and $d_t(m) \triangleq [y_t - e^{j\frac{m\pi}{4}}]^2$ is the Euclidean distance between received signal $y_t$ and the constellation point $C_m$. Afterwards, the LLR could be

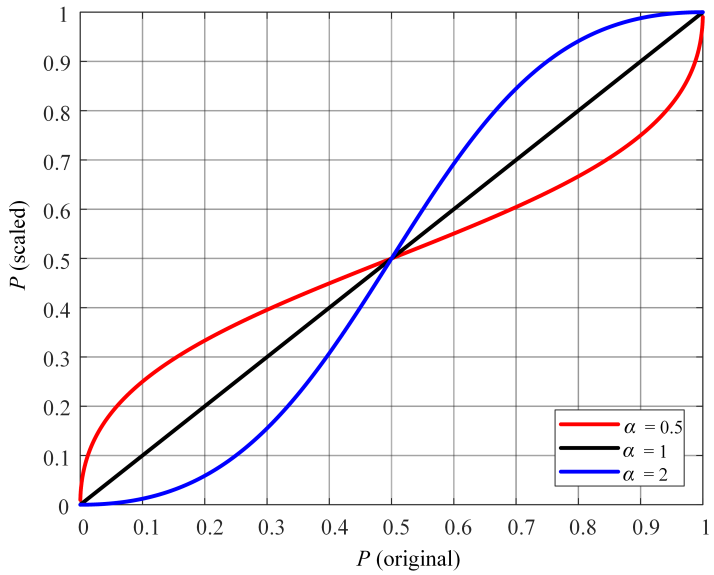



Figure 3–9: The scaling operation with scaling factor $\alpha = 0.5, 1, 2$.

calculated as,

$$\begin{aligned} LLR_t(b_1) &= \log \frac{P(b_1 = 0)}{P(b_1 = 1)} = \log \left[ \frac{P_t(\frac{\pi}{4}) + P_t(\frac{5\pi}{4})}{P_t(\frac{3\pi}{4}) + P_t(\frac{7\pi}{4})} \right] \\ &\approx \frac{\max\limits_{k,l} \left[ d_{t-1}(k) + d_t(k+3), d_{t-1}(l) + d_t(l+7) \right]}{N_0} \\ &- \frac{\max\limits_{k,l} \left[ d_{t-1}(k) + d_t(k+1), d_{t-1}(l) + d_t(l+5) \right]}{N0}. \end{aligned} \tag{3.17}$$

where $k, l = 0, 1, ..., M-1$. The other bit LLR $LLR_t(b_2)$ could be calculated in the similar way. The log-likelihood ratio would be passed to stochastic BCH decoder.

Using the max-log approximation method, there would be no $\exp(\cdot)$ operation involved. The division operation $\frac{1}{N_0}$ could be eliminated by the NDS method. Thus, the soft-decision demodulation for $\frac{\pi}{4}$-DQPSK shows an acceptable complexity.

**Noise-dependent scaling**

For many of the stochastic computing based decoders, to reduce the number of hold states, NDS [87] is used to reduce the error floor and speed up convergence:

$$LLR_n^{'} = \alpha \cdot LLR_n, \tag{3.18}$$

where $\alpha = \lambda \cdot N_0$ is the scaling factor obtained through simulation, and $N_0$ is the noise power, while usually $\alpha < 1$. The scaling result is demonstrated as red curve in Figure 3–9.

The scaling operation on the soft input is used to narrow the searching range and reduce the decoding latency. As illustrated in Figure 3–9 (blue curve), the linear scaling operation on the $LLR_n$ results in a non-linear scaling operation on the original probability. The highly reliable inputs, such as $P_n > 0.9$ and $P_n < 0.1$, are scaled close to 1 and 0, respectively. Based on the fact that the error bits usually occurs at low reliable positions, smaller searching range leads to a lower decoding latency. Moreover, by using the NDS method, there is no need for noise power estimation for soft decision demodulation module.

### 3.5.4 Evaluation and implementation of the proposed stochastic computing based decoder for BCH codes in WBAN systems

In this section, the simulation results on decoding performance, decoding latency analysis, and hardware implementation results are presented.

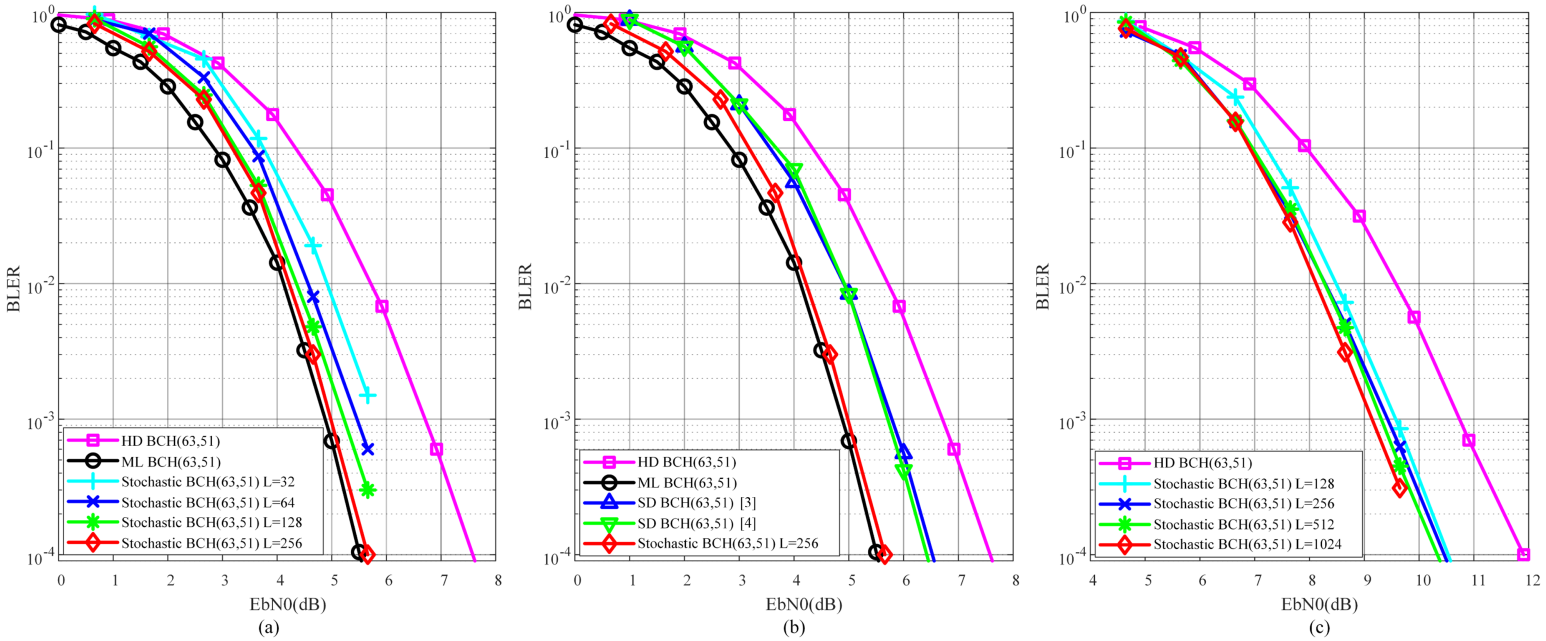



Figure 3–10: (a) BLER simulation results for the (63,51,2) BCH code defined in IEEE 802.15.6 standard. (b) Decoding performance comparison between the proposed stochastic SDD and the existing SDD BCH decoders. (c)Decoding performance comparison between the proposed stochastic SDD and the conventional HDD for WBAN system with $\frac{\pi}{4}$-DQPSK modulation.

**Performance simulation**

The proposed stochastic BCH decoder is simulated based on a BPSK modulated communication system with the (63,51,2) BCH code specified in the IEEE 802.15.6 standard. The floating point ML decoder and HDD [39] are also plotted in Figure 3–10 (a) for comparison. The length of the bit streams $L$ in the proposed stochastic BCH decoder is set to 32, 64, 128, and 256 respectively. It can be observed that the performance of the proposed stochastic BCH decoder improves significantly with the increase of bit stream length. Eventually, it approximates to the performance of floating point ML decoder when $L = 256$, with only 0.1 dB loss. In the rest of the simulation and implementation for WBAN system with BPSK modulation, the bit stream length $L$ is selected to be 256.

As demonstrated in Figure 3–10 (b), a comparison between proposed stochastic BCH decoder and existing soft-decision BCH decoders [45], [110] has been illustrated. It can be observed that the proposed stochastic BCH decoder outperforms the existing SD decoders by 1 dB in terms of Eb/N0. Moreover, the proposed design provides 1.75 dB coding gain compared to HDD.

Further, to adopt the proposed stochastic BCH decoder to the IEEE 802.15.6 standard, a practical WBAN system with $\frac{\pi}{4}$-DQPSK modulation is simulated. The decoding performance is illustrated in Figure 3–10 (c). Compared with the HDD decoder, the proposed stochastic BCH decoder with bit stream length $L = 1024$ gains 1.75 dB at BLER=$10^{-3}$, which means that 33% transmission power could be saved for a practical WBAN system.

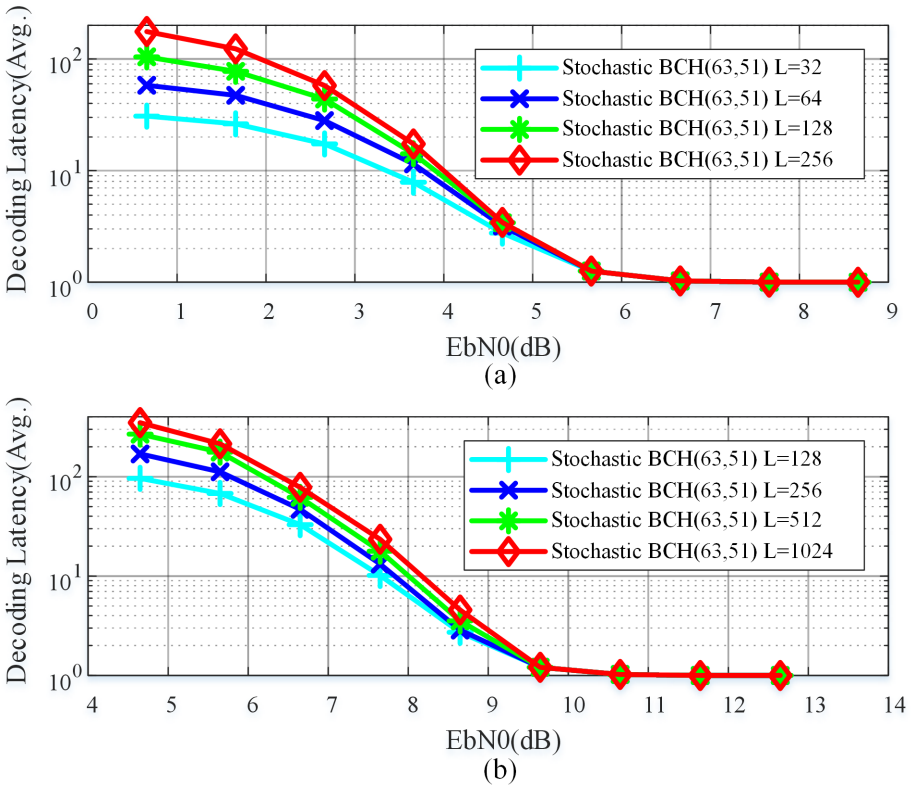



Figure 3–11: (a) Average decoding latency of the proposed stochastic BCH decoder with CRC aided early stopping criteria, where $L = 32, 64, 128, 256$ and BPSK modulation. (b) Average decoding latency of the proposed stochastic BCH decoder with CRC aided early stopping criteria, where $L = 128, 256, 512, 1024$ and $\frac{\pi}{4}$-DQPSK modulation.

**Latency evaluation**

Benefiting from the CRC aided early stopping criteria, the proposed stochastic BCH decoder illustrates a significantly reduced decoding latency at high signal-to-noise ratio region. The IEEE 802.15.6 standard requires the frame error rate lower than 10%, where each frame consists of 1∼255 Bytes (up to 40 BCH code blocks). Thus, in a practical WBAN system, the proposed stochastic BCH decoder would work at the Eb/N0>4.5 dB region (BLER<$10^{-2}$), where it takes lower than 4 clocks latency on average shown as Figure 3–11 (a).

In addition, the stochastic BCH decoders with bit streams length $L = 32, 64, 128, 256$ show a similar average decoding latency when Eb/N0>4.5 dB which means a longer bit stream length would lead to much better decoding performance with little deterioration on decoding latency.

For a practical WBAN system with $\frac{\pi}{4}$-DQPSK modulation, the average decoding statistics are plotted in Figure 3–11 (b). Even though the maximum bit stream length is relatively long, the stochastic BCH decoding converges quite fast, lower than 2 clock cycles at Eb/N0>9 dB, where BLER is lower than $10^{-3}$.

**Hardware implementation**

Table 3–3: Comparison of (63,51,2) BCH code in IEEE 802.15.6 hardware implementations.

| Design | Hard-Decision [110] | Soft-Decision [110] | Soft-Decision [45][a] | Stochastic Decoder [This work][e] |
|---|---|---|---|---|
| CMOS Technology (nm) | 90[d] | 90[d] | 90 (TSMC) | 90 (TSMC) |
| Code ($N$, $K$, $t$) | (63,51,2) | (63,51,2) | (63,51,2) | (63,51,2) |
| Coding Gains[b] | 0 dB | 0.75 dB | 0.75 dB | 1.75 dB |
| Clock Frequency (MHz) | 143 | 66 | 250 | 281 |
| Logic Gates | 9618 | 16698 | 6171 | 16321 |
| Area ($um^2$) | 35140 | 34768 | 17416 | 33983 |
| Average Latency[c] (clock cycles) | 1 | 1.4 | 9 | 2 |
| Throughput[c] (Mbps) | 7283 | 2365 | 1417 | 7165 |
| Hardware Efficiency (Mbps/K Gates) | 432 | 50 | 230 | 439 |

[a]The parallelism level is selected as 7 (defined as decoding bits in one clock cycle), which is reported the highest hardware efficiency in [45]. [b]Measured at BLER=$10^{-2}$ with BPSK modulation compared to HDD performance. [c]Measured at Eb/N0=5dB. [d]The CMOS technology is not detailed in [110]. [e]For fair comparison, the soft-decision demodulation for $\frac{\pi}{4}$-DQPSK is not included in the synthesis results.

Form Table 3–3, it can be observed that the area consumption and logic gates of the proposed design is lower than the existing SDD [110] as a result of the simple architecture of stochastic computing. The SDD in [45] shows the lowest hardware cost due to its lower parallelism level ($P = 7$). The design in [110] and [45] used a test syndrome calculation and sorting module with complex structure and longer delay, resulting in a lower throughput than proposed work. Consequently, compared to the conventional binary system based SDD, the proposed design illustrates the advantages of both coding gains and the hardware efficiency defined as the ratio of throughput to logic gates.

### 3.5.5 Conclusions of the proposed stochastic computing based decoder for BCH codes in WBAN systems

This section presents a novel stochastic computing based decoder for BCH codes in WBAN systems. A combinational logic based hard decision decoding kernel and noise-dependent scaling are characterized in the proposed design to further reduce the hardware cost and improve the throughput, which contributes to high hardware efficiency. Besides, the soft-decision $\frac{\pi}{4}$-DQPSK demodulation method is adopted in this design to provide the log-likelihood ratio for the proposed stochastic BCH decoder. The proposed decoder significantly improves the decoding performance with respect to the existing art in soft decision decoders, while achieves higher area efficiency. The proposed stochastic BCH decoding scheme could be a good implementation candidate for practical WBAN systems.

## 3.6 Summary of the chapter

With the development of advanced sensors, increasing types of human biomedical data can be collected accurately. However, most of the communication between

biomedical sensors and centralized devices are still utilizing existing wireless protocols such as Bluetooth or Zigbee, even though the IEEE 802.15.6 WBANs standard has specified the communication methods in WBANs. A significant reason for that situation is that few baseband processing modules had been proposed for WBANs. An ASIC of such a baseband processing module in NB physical layer for WBANs based on IEEE 802.15.6 WBANs standard has been proposed in this chapter. By comparing the performance with other publications, the proposed ASIC for baseband processing demonstrates advantages in multiple perspectives. Meanwhile, to further reduce the power consumption of the baseband processing module of WBANs, a novel stochastic computing based BCH decoder has been proposed and evaluated in this chapter, which has been proved that the proposed design has advantages in better wireless communication performance, lower power consumption, and better fault tolerance ability.

# CHAPTER 4
# Security Techniques for WBANs and Corresponding Hardware Implementations

With the development of WBANs and sensors, various types of biomedical data such as ECG [84], heart rate [14], and blood pressure[112] of the user, can be collected conveniently and accurately as illustrated in Table 1–1. Moreover, some nodes such as the smart insulin pumps mentioned in [119] have a feedback system. The behavior of the node is based on the current situation of the user and the analysis of the system. Therefore, maintaining security in WBANs becomes a significant research topic, as the networks are transferring more and more critical data [56].

In the IEEE standard 802.15.6 for WBANs, security requirements have been determined and regulated [51]. Based on the standard, various algorithms and implementations of security schemes [27][118][116][72][80][6][77] have been proposed. The majority of the above papers are focusing on the software implementation of their proposed solutions. [77] proposed an optimized general microprocessor design which has special functional units and instructions integrated, resulting in accelerated Advanced Encryption Standard (AES) encryption. Meanwhile, [6] evaluated their proposed security scheme in a Field-Programmable Gate Array (FPGA). Previous work will be reviewed and discussed in detail in the section of background and previous work.

In this chapter, a security scheme for WBANs and corresponding ASIC implementation are proposed based on the requirements of the IEEE 802.15.6 WBANs standard. It contains an authentication module, an ECC encryption module, and another logic control unit. Furthermore, to further reduce the power consumption and increase the security level of the encryption module of WBANs, a novel dynamic encryption method based on the characteristic values of the body channel has been discussed in this chapter. It decreases the system complexity of the encryption module and utilizes dynamic encryption to increase security protection.

## 4.1 Background and previous work

As mandated by the IEEE standard 802.15.6, three security levels (Level 0, Level 1, and Level 2) have been specified to classify the communication process [51]. The security level of a specific communication is determined by data type and privacy level. For the lowest security level (Level 0), the plaintext is directly transmitted, and no authentication is required. In the case of Level 1, authentication is required before the node gets access to the network while the data transmission is still in plaintext. The communication of security Level 2 requires both authentication and encryption, such as ECC, which provides the highest protection in WBANs. On the basis of the security and power constraints of WBANs, light-weight data authentication schemes have been proposed in [27] and [80]. Compared to other proposed protocols such as SPINS and BROSK, these schemes achieved up to 98% and 67% less power consumption respectively. It makes them more feasible in nodes side which is limited by the power supply and computational ability. Moreover, ECG and other biomedical data are involved as dynamic factors in the design schemes of [116] and

[72]. Biomedical data is utilized to generate keys used for data authentication and encryption. This method simplifies the system while maintaining its security level and properties.

In terms of hardware implementation, [6] designed and implemented an FPGA-based hardware security add-on solution for WBANs. [77] proposed a security scheme for WBANs operated on a custom microprocessor optimized for AES encryption. It integrated vector functional units and cryptography instructions to accelerate the process of the encryption.

## 4.2 Proposed security scheme for WBANs

According to the specifications of the IEEE 802.15.6 standard, authentication needs to be done by the validation of the certificate. The method of encryption for the communication is ECC. However, the detailed implementation methods, such as the method of validation procedure, are not clarified in the standard.

The proposed security scheme consists of four major hardware modules: the authentication module, encryption module, an interface between the authentication and encryption module, and an interface for the security scheme. The authentication and encryption module could work independently or together, depending on the security level of the communication. For instance, both authentication and encryption modules are enabled when the security level of the communication is Level 2. A diagram of the proposed security scheme is demonstrated in Figure 4–1, while the sequence is illustrated in Figure 4–2. Serial Peripheral Interface (SPI) has been utilized as the interface of the security scheme for establishing the connection between the proposed security scheme and existing systems.

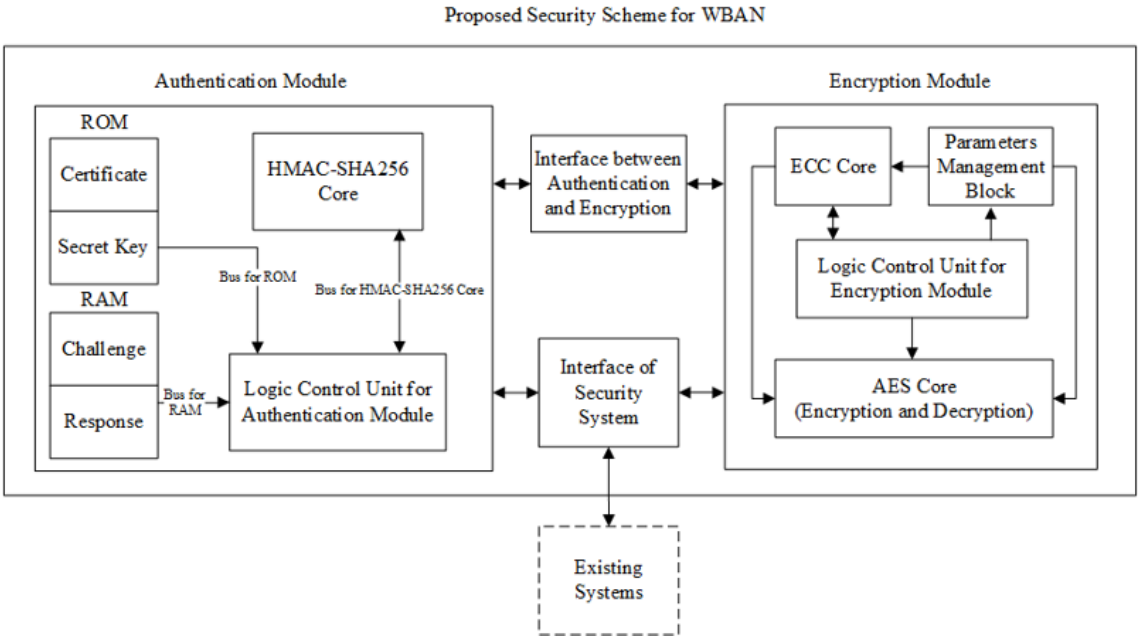



Figure 4–1: Proposed security scheme for WBANs

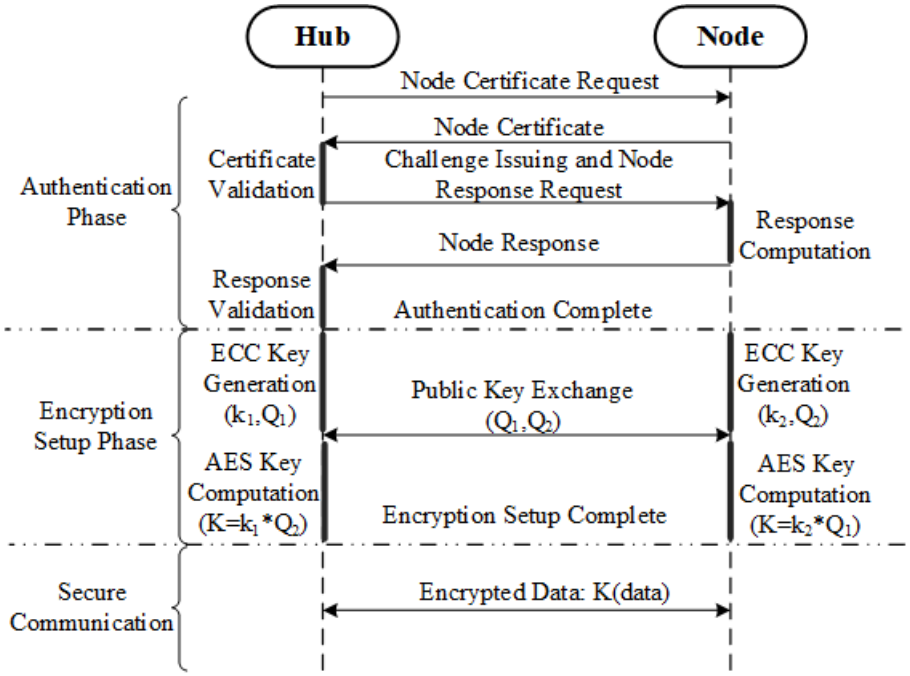



Figure 4–2: Sequence of proposed security scheme

### 4.2.1 Proposed authentication module

The procedure of the proposed authentication method can be broken down into two steps: i) validation of a certificate and ii) validation of the challenge-response exchange. The sequence of the authentication phase is illustrated in Figure 4–2.

**Validation of certificate**

As mentioned previously, the certificate validation is a procedure that has been specified in the standard IEEE 802.15.6. However, there are multiple methods for achieving the requirements of the standard. In the proposed design, validation of certificate involves an X.509 certificate [26] and two tasks are performed here. First, the certificate, found in the unknown node, is sent to the Hub. Second, the certificate is validated by the Hub. The certificate obeys the X.509v3 standard. A certificate chain can be found in the Hub with the node certificate signature verified using the public key of the next certificate. For testing purposes, the certificates used were self-signed and generated using OpenSSL. Validity is accomplished by following the certification path validation algorithm, as specified by RFC 5280 [26]. Once the certificate is validated, the certificate-holding node is genuine. In the username-password authentication equivalent, the username has now been provided and it is trusted. The password security layer in the form of challenge-response authentication is next. It secures the system further by explicitly tying unique challenge responses to nodes and requesting them on authentication.

**Validation of challenge-response exchange**

Validation of the challenge-response exchange is an additional security procedure that is not specified in the standard IEEE 802.15.6. It is broken down into three

steps. Initially, a 64 bits challenge is generated by the trusted hub. The challenge can be considered as a random sequence of bits, and can potentially be generated using biomedical data collected by connected nodes such as ECG, temperature, and blood pressure. The challenge is sent to the unknown node where it is processed. A 256-bit response is computed using a 256-bit secret key only known to the trusted hub and trusted nodes. Then, the response is sent back to the hub, which computes the response using the same procedure and compares it with the received one.

To compute the response, the Hash-based Message Authentication Code (HMAC) is involved. The HMAC is a secure procedure which is based on a cryptographic hash function. In this case, the hash function utilized is Secure Hash Algorithm-256 (SHA-256). Any weaknesses found in the underlying hash function inherently become weaknesses of the message authentication code. For this reason, the function needs to be resistant to attacks (for instance collisions) [49].

In short, hash functions work by mapping an arbitrarily large set of inputs into a typically smaller fixed set of outputs. This output set is generated procedurally but differs a lot from the input and cannot be traced back. A collision happens when two inputs can give exactly the same output. This is also known as birthday problem [99]. This is extremely unlikely to happen accidentally. However, flaws in the hash functions can make it possible to detect collisions and forge messages to deliberately cause them. Popular functions such as MD5 or SHA-1 have been determined to be insecure, as shown by the Software Engineering Institute in Carnegie Mellon University [28], and by the CWI Institute in Amsterdam and Google [83], respectively. For this reason, the hash function SHA-256, which is considered to be a safer alternative,

was used in the proposed authentication module, which is considered to be a safer alternative.

The HMAC procedure works in such a way that it combines two inputs, a message ($m$) and a secret key ($k$), and produces an output, HMAC($m, k$), with the use of a hash function ($H$). The hash function is executed twice, and is a functional block of the HMAC, together with addition modulo 2 operations (XOR) and concatenation. The procedure is shown in equation 4.1, with $\oplus$ and $|$ indicating XOR and concatenation respectively.

$$HMAC(m,k) = H\Big(\big(k \ \oplus \ opad\big)|H\big(\,(k \ \oplus \ ipad)\,|m\big)\Big) \tag{4.1}$$

The *ipad* and *opad* are inner and outer padding constants, and consist of the repeating values 0x5c5c.. and 0x3636.. extended to the length of the hash block size. A similar pre-processing is performed on the key, which is shorter. It is padded with zeros on the right to match the length of the hash block size. If the key happens to be longer, the hash function is executed a third time on the key itself, to reduce the key length to the correct length.

As shown, the pre-processed key is initially XOR-ed with the inner padding, and the output of that is concatenated with the message, all of which is hashed. The pre-processed key is then XORed with the outer padding, and concatenated with the output of the aforementioned hash. The output of the concatenation will be hashed again, and the output of the hash function this time is the final output.

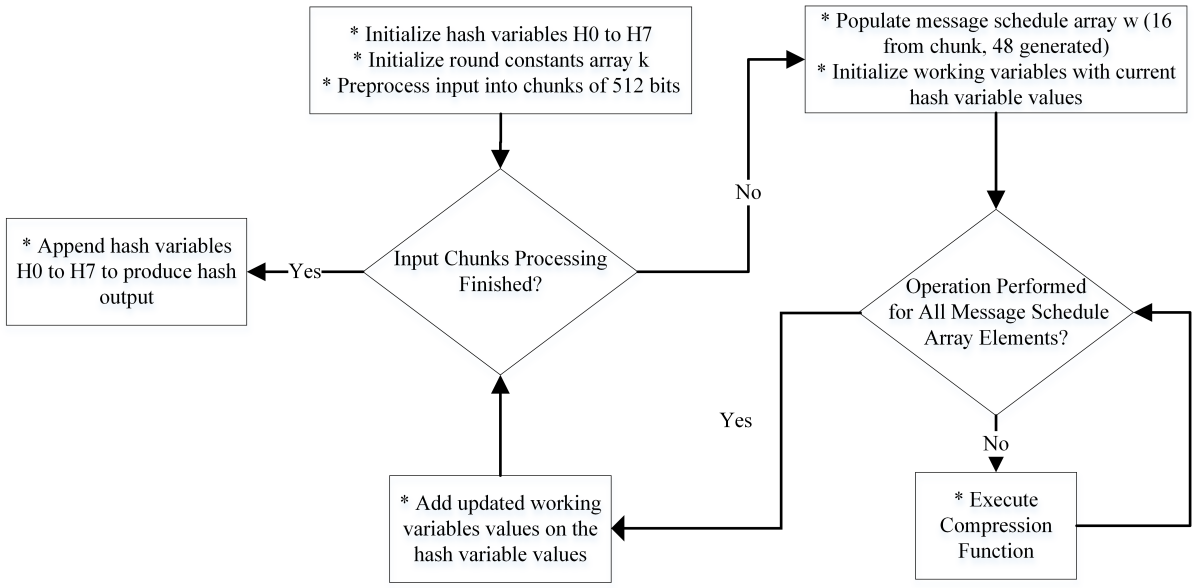



Figure 4–3: Flowchart of SHA-256

As mentioned, any hash function can be used to implement the $H$ block, and in this case, it is SHA-256. The procedure of SHA-256 is illustrated briefly in Figure 4–3.

SHA-256 begins by initializing 8 variables, hash variables $H_0$ to $H_7$, with the first 32 bits of the fractional parts of the square roots of the first 8 prime numbers, 2 to 19. Variables $H$ are used to store the hash output. Another initialization follows, which initializes an array, $k$, with 64 constants ($k_0$ to $k_{63}$). These constants, also called round constants, are the first 32 bits of the fractional parts of the cube roots of the first 64 prime numbers, 2 to 311.

After initialization, some pre-processing is performed on the hash input. A single '1' bit is appended to the end at first. Then, a number of '0' bits are appended, such that $L + 1 + K + 64$ is a multiple of 512, with L being the length of the input, 1

the '1' bit, and $K$ the number of '0' bits appended. Once that is done, the length $L$ is appended to the end as a 64-bit big-endian integer, hence the value 64, bringing the total length to a multiple of 512. The message is then broken down into chunks of 512 bits, with the following procedure utilizing variables $H$, repeating for each chunk, and adding back to the variables $H$ for every iteration. Evidently, if the hash input is relatively small, the function will only execute for one chunk.

For every chunk, an array, w, needs to be created and populated. The array is also called a message schedule array, and much like the round constant array, it contains 64 32-bit elements. To populate the array, the chunk is broken down into 16 32-bit sub-chunks, which are copied on the first 16 elements of the message schedule array, w0 to w15. For the remaining 48 elements, equation 4.2 shows how they are populated. It should be noted that ROR indicates rotating to the right, that is, the bits dropped are placed on the space created on the left, whereas SHR indicates shifting to the right, that is, the bits dropped are discarded and the space created is populated with '0' bits.

$$w_i = w_{i-16} + w_{i-7} + S_0 + S_1 \tag{4.2}$$

where

$$\begin{aligned} S_0 &= (w_{i-15}\ ROR\ 7)\ \oplus\ (w_{i-15}\ ROR\ 18)\ \oplus\ (w_{i-15}\ SHR\ 3) \\ S_1 &= (w_{i-2}\ ROR\ 17)\ \oplus\ (w_{i-2}\ ROR\ 19)\ \oplus\ (w_{i-2}\ SHR\ 10) \end{aligned} \tag{4.3}$$

The next step is to initialize 8 temporary working variables, a to h, with the contents found in the hash variables $H_0$ to $H_7$. Then, for every element of the

message schedule array (total of 64) a compression function is executed, which will manipulate the temporary working variables. The algorithm of the function is shown below, in equations 4.4 to 4.6.

$$\begin{aligned} h &= g,\ g = f,\ f = e,\ e = d + T_1 \\ d &= c,\ c = b,\ b = a,\ a = T_1 + T_2 \end{aligned} \tag{4.4}$$

where

$$\begin{aligned} T_1 &= h + S_1 + ch + k_i + w_i \\ T_2 &= S_0 + maj \end{aligned} \tag{4.5}$$

where

$$\begin{aligned} S_1 &= (e\ ROR\ 6)\ \oplus\ (e\ ROR\ 11)\ \oplus\ (e\ ROR\ 25) \\ ch &= (e\ \&\ f)\ \oplus\ (\bar{e}\ \&\ g) \\ S_0 &= (a\ ROR\ 2)\ \oplus\ (a\ ROR\ 13)\ \oplus\ (a\ ROR\ 22) \\ maj &= (a\ \&\ b)\ \oplus\ (a\ \&\ c)\ \oplus\ (b\ \&\ c) \end{aligned} \tag{4.6}$$

As can be seen, the compression function relies on $i$, which is an element of the round constants ($k_i$) and message schedule ($w_i$) arrays. Following the compression function, the working variables will be added back to the hash variables, updating their value. This procedure will repeat until there are no more chunks left to process, at which point, the output of the hash is simply the hash variables appended to each other as shown in equation 4.7.

$$H = H_1|H_2|H_3|H_4|H_5|H_6|H_7 \tag{4.7}$$

### 4.2.2 Proposed encryption module

#### Elliptic curve cryptography

ECC is utilized as the cryptography method for the proposed encryption module. ECC is an efficient cryptography approach; it has been proven that it can achieve the same security level as other public-key cryptography methods, by using a much shorter key size [47] [13] [104]. Because of that, and the advantages of lower power consumption, lower processing latency, and lower memory consumption, ECC is accepted by IEEE 802.15.6 standard as a standard encryption scheme [89].

ECC was proposed as an alternative public-key system to provide stronger security compared to the established Rivest, Shamir, and Adelman (RSA) and Digital Signature Algorithm (DSA) system [30] [48] [63]. The reason stronger security cryptography is needed is that the integer factorization problem and discrete logarithm in the existing RSA and DSA take sub-exponential time. With the increasing computational ability, an ever-increasing key is needed to provide enough safety. For example, it is suggested to select 1024-bit long keys in the standard established by the National Institute of Standards and Technology (NIST) [35].

In contrast to that, the security of ECC is mainly based on the apparent intractability of Elliptic Curve Discrete Logarithm Problem (ECDLP); given an elliptic curve $E(F_q)$, a base point $P \in E(F_q)$, and an order $k$, it is easy to calculate another point on the elliptic curve with the point-multiplication defined on the finite field $F_q$. $Q = k \cdot P = \underbrace{P + P + \cdots + P}_{k\ times} \in E(F_q)$, where $k$ could be used as the private key, and $Q$ could be used as the public key.

The basic attack on ECC is calculating the order $k$, which is used as the private key, from these two given points $P$ and $Q$, provided that such integer exists. However, even the most efficient general algorithm will be tremendously complex to compute (exponential to the order key size) [35] [71] [106]. Consequently, the main attractive point of ECC over the existing technologies is that the best algorithm to solve the underlying hard mathematical problem, the ECDLP, takes fully exponential time in ECC. It is proven that the ECC public-key systems with 160-bit keys provide an equivalent level of security to the existing RSA and DSA systems with 1024-bit keys [8]. The lack of a sub-exponential attack on ECC offers potential reductions in processing power, storage space, bandwidth, and electrical power. These advantages make ECC a better cryptography candidate for constrained devices such as smartphones and IoT devices.

**The Mathematics behind ECC**

In general, an elliptic curve is the set of points described by the equation:

$$y^2 = x^3 + ax + b \tag{4.8}$$

where $4a^3 + 27b^2 \neq 0$. The curves may have different shapes on the plane based on the value of $a$ and $b$. Meanwhile, assume a point at infinity which is represented by the symbol of 0(zero). Then the definition of the elliptic curve now is

$$\left\{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 \neq 0\right\} \cup \{0\} \tag{4.9}$$

There are four group laws applied in elliptic curves:

1. The elements of the group are the points of an elliptic curve;

2. The identity element is the point at infinity 0;

3. The inverse of a point $P$ is symmetric about the x-axis;

4. The addition is given by the following rule: given three aligned, non-zero points $P$, $Q$, and $R$, their sum is $P + Q + R = 0$

If we draw a line passing through two separated points $P$ and $Q$, this line will intersect a third point on the curve, $R$. If we take the inverse of this point, $-R$, then it is the result of $P + Q$, since that is the group law for elliptic curves. If $P$ and $Q$ are distinct, the slope of the line through them is

$$m = \frac{y_P - y_Q}{x_P - x_Q} \tag{4.10}$$

The intersection of this line with the curve is $R = (x_R, y_R)$ where

$$x_R = m^2 - x_P - x_Q \tag{4.11}$$

$$y_R = y_P + m(x_R - x_P) \tag{4.12}$$

When $P = Q$, the slope of the curve is defined as:

$$m = \frac{3x_P^2 + a}{2y_P} \tag{4.13}$$

this expression for $m$ is the first derivative of:

$$y_P = \pm\sqrt{x_P^3 + ax_P + b} \tag{4.14}$$

Besides addition, there is another operation in the elliptic curve which is scalar multiplication defined as follow:

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ times}} \tag{4.15}$$

where $n$ is a natural number. As can be seen, computing $nP$ requires $n$ additions, and assume that $n$ has $k$ binary digits, then the algorithm is $O(2^k)$, which is relatively complicated.

One example of the faster algorithms for scalar multiplication is double and add algorithm. An example is given to illustrate the algorithm. Assume $n = 151$ which is 10010111 in binary. Then,

$$151 \cdot P = 2^7P + 2^4P + 2^2P + 2^1P + 2^0P \tag{4.16}$$

Based on the algorithm, it can be computed as following:

1. Take $P$ and double it so that we can get $2P$;
2. Add $2P$ to P, so that we can get $2^1P + 2^0P$
3. Double $2P$, so that we can get $2^2P$
4. Add it to the previous result, so that we can get $2^2P + 2^1P + 2^0P$
5. Double $2^2P$ to get $2^3P$
6. Do not perform any addition involving $2^3P$
7. Double $2^3P$ to get $2^4P$
8. Add it to the previous result, so that we can get $2^4P + 2^2P + 2^1P + 2^0P$
9. ...

n. ...

By utilizing this double and add algorithm, it is feasible to compute $Q$ based on $n$ and $P$. However, it is extremely difficult to do the other way. It means it is extremely difficult to compute $n$ based on $P$ and $q$, which is also known as the logarithm problem.

Since the computer has limited memory and computing ability, it is necessary to restrict the elliptic curves to finite fields. A finite field is a set with a finite number of elements. An example of the finite field is the set of integers modulo $p$, where $p$ is a prime number, which is denoted as $GF(p)$ or $\mathbb{F}_p$. The set of integers modulo $p$ contains all the integers from 0 to $p-1$. Therefore, the elliptic curves in the $\mathbb{F}_p$ can be expressed as:

$$\begin{aligned} &\{(x,y) \in (\mathbb{F}_p)^2 | y^2 \equiv x^3 + ax + b \pmod{p}, \\ &4a^3 + 27b^2 \not\equiv 0 \pmod{p}\} \cup \{0\} \end{aligned} \tag{4.17}$$

For the point additions in the finite field, it is similar to the previous procedure, while just need to add "mod p" at the end of each expression. For a given $P$ and $Q$, for computing the $-R$, the slope is:

$$m = (y_P - y_Q)(x_P - x_Q)^{-1} \tag{4.18}$$

and the $x_R$ and $y_R$ are:

$$\begin{aligned} x_R &= (m^2 - x_P - x_Q) \bmod p \\ y_R &= [y_P + m(x_R - x_P)] \bmod p = [y_Q + m(x_R - x_Q)] \bmod p \end{aligned} \tag{4.19}$$

In term of the point multiplications in finite filed, the double the add algorithm also works. Meanwhile, the multiplications are repeating cyclically. For every integer $k$,

$$kP = (k \bmod 5)P \tag{4.20}$$

**Curve25519 for ECC**

Since different curves utilized in ECC lead to different performance for the encryption module, a certain proper curve of ECC for the proposed encryption module shall be determined based on the requirements of WBANs.

Curve25519 is a function to accelerate the Diffie-Hellmann key agreement over elliptic curves. It is based on a prime field with a prime number close to a power of 2 (Pseudo Mersenne Prime) and defined over prime fields $GF(p)$, where let p be a prime number with $p > 3$ and $F_p = GF(p)$ the Galois Field over p. The curve is specified as following [75]:

$$Y^2 = x^3 + 486662x^2 + xmod(2^{255} - 19) \tag{4.21}$$

Assume a base point $P$ with $Q = (X_i, Y_i, Z_i)$. It defines a combined point doubling and point addition functions as a single step of the Montgomery Power ladder [64] with 4 squares, 5 general multiplications, 1 multiplication by (A-2)/4 and 8 additions or subtractions. Meanwhile, since only x-coordinate of each point is necessary for the computing in the Curve25519, y-coordinate can be omitted in the formulas. Thus, the point multiplication only relies on the x and z coordinates of the two points $Q$ and $Q'$. Therefore, the combined step can be computed by the following equations

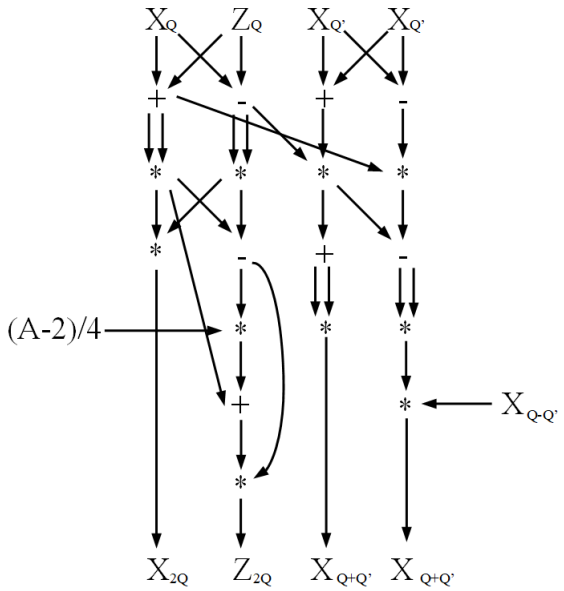



Figure 4–4: Double and add formula based on Montgomery's ladder

[75].

$$
\begin{aligned}
x_{2Q} &= (x^2 - Z^2)^2 = (x - z)^2(x + z)^2 \\
z_{2Q} &= 4xz(u^2 + Axz + z^2) \\
x_{Q+Q'} &= 4(xx' - zz') \\
z_{Q+Q'} &= 4(xz' - zx')x_1
\end{aligned}
\tag{4.22}
$$

In term of scalar multiplication $k \times P$ on the curve, there are 255 combined point double and addition operations are performed followed by a final inversion and single multiplication calculating $X \times Z^{-1}$. The algorithm is illustrated in Figure 4–4.

In the proposed encryption module, Curve25519 has been utilized as the curve for ECC, which is a state-of-the-art ECDH function suitable for a wide variety of

cryptographic applications. There are multiple advantages of the Curve25519 [12] as illustrated below which is suitable for the circumstances of WBANs applications.

1. Free key validation. In typical ECDH encryption cases, the public keys must be validated at the initial phase for encryption since the functions could be broken down once the public key is not a point of order $n$ in $E(F_q)$, where $F_q$, $E$, and $n$ are specified by the corresponding domain parameters [4]. In other words, extra hardware resources are required for the public key validation purpose, which also leads to relatively noticeable latency for the encryption module. However, the validation procedure for the public key is not needed for Curve25519 since every 32-byte string is accepted as a Curve25519 public key.

2. No time variability. As one of the most popular attack methods for side-channel attacks, the goal for timing attack is to analyze what types of logic computations have been done in the encryption block by measuring the latency of various computations takes to perform for different inputs. However, Curve25519 is immune to timing attacks, including hyperthreading attacks and other cache-timing attacks, because it avoids all input-dependent branches, all input-dependent array indices, and other instructions with input-dependent timings [12].

3. Not patented. Even though there are multiple curves could be selected potentially to perform the ECC for the encryption module, while most of them are patented such as US patent 5159632, US patent 5271061, and US patent 5463690. However, Curve25519 is a public curve to the scientific community, which allows us to dig into it.

4. High execution speed. By utilizing Curve25519, the experiment result of ECC illustrates that it is one of the fastest ECC curves have been released [12].

Due to the unique algorithm of the Curve25519, it provides multiple characteristics facing the side channel attacks. Precisely, the timing attack is one of the most popular attack methods for discovering the secret stored in a certain block by finding dependencies between the secret and the operation time of the cryptographic computations. However, as demonstrated in Figure 4–4, every addition or subtraction is followed by multiplication and almost every multiplication is followed by an addition or subtraction. Meanwhile, regardless of the data, the number of operations executed is always the same for Curve29915. Therefore, the Curve25519 can prevent timing attacks by its own natural advantages.

Similar to timing attacks, the goal for Simple Power Analysis (SPA) is to reveal a secret by measuring and inspecting the instantaneous power consumption of a device during the cryptography computing operation depending on the secret. However, since Montgomery's Ladder of Curve25519 has the advantage of same numbers of operations during the computing procedure, the power consumption of is always identical, which means SPA can also be prevented.

In term of the hardware architecture of Curve25519 core, based on the mathematical algorithm of the Curve29915 provided by [12], the hardware architecture of Curve25519 core [75] is illustrated in the Figure 4–5. The core is mainly constructed by four modules, which are modular addition unit, modular multiplication unit, a RAM, and a logic control unit. To be more precise, the responsibility of modular addition unit is to compute the modular addition and subtraction of $c = a \pm b \; mod \; (p)$

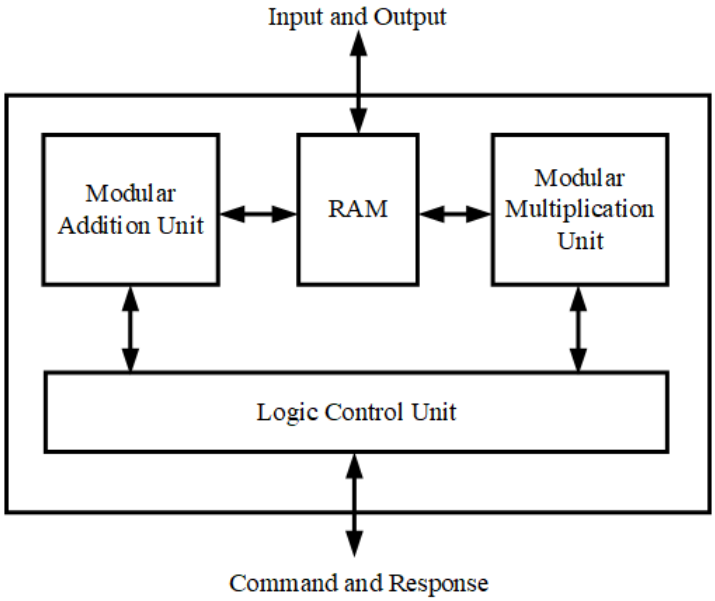



Figure 4–5: Curve25519 core

by two blocks of digital signal DSPs which supports addition, subtraction, multiplication, and accumulation, while one of the DSP is performing the computation of $c^{'} = a \pm b$ and the other one is computing the $c^{''} = c^{'} \mp p$. The result of the computation coming from the two DSPs is stored in the RAM. In term of the modular multiplication unit, it contains 18 DSP modules, 15 of them are utilized for computing the partial production, one of them are used for pre-reduction, and the last two for the final modular reduction. Same as the modular addition unit, the results are stored in the RAM of the core. The logic control unit oversees the control signal (command and response) internally and externally.

**AES-ECC encryption system**

AES is a stronger symmetric-key algorithm compared to the previous Data Encryption Standard (DES) scheme, which is selected by NIST [29].

In this design, the ECC and AES techniques are combined to achieve a strong and efficient encryption scheme in the proposed security scheme. In this scheme, the ECC module generates and exchanges the public key based on the Elliptic-Curve Diffie-Hellman (ECDH) key agreement protocol [9]. Using the secured channel, a shared key is generated and exchanged between both communication ends, and faster symmetric encryption ensues, as performed by the AES module. The hardware structure of the proposed encryption module is shown on the right side of Figure 4–1.

The encryption procedure of the module is illustrated as follows: At the very first, the random private keys are generated on both communication ends, which are marked as k1 and k2, respectively. Using the ECC module, both sides calculate the public key as

$$Q_1 = k_1 * P \tag{4.23}$$

$$Q_2 = k_2 * P \tag{4.24}$$

where P is a base point pre-defined on the elliptic curve. The multiplication operator is a point multiplication defined on the elliptic curve. The safety of the ECC encryption is guaranteed by the ECDLP; it is extremely hard to calculate k from Q and P. According to the ECDH protocol, the public keys Q1 and Q2 can be shared between both sides.

$$
\begin{aligned}
K &= k_1 * Q_2 \\
&= k_1 * (k_2 * P) \\
&= k_1 * k_2 * P \\
&= k_2 * (k_1 * P) \\
&= k_2 * Q_1
\end{aligned}
\tag{4.25}
$$

Finally, the symmetric key is generated as shown in Equation4.25, which can be used in AES to encrypt and decrypt the plain text. The ECDH based key agreement is only processed once before the whole authentication procedure.

For the AES module, a counter operation mode (AES-CTR) is selected. One of the reasons is that AES-CTR provides strong safety in the block encryption. The other reason is that the encryption and the decryption could share the same hardware module, which is significant for the low power requirements of the WBANs.

The middle part of Figure 4–2 demonstrates the sequence of the encryption setup phase. After that, the communication between the nodes and Hub is secured.

## 4.3 Evaluation of the proposed security scheme in FPGA

The proposed security scheme was implemented with Verilog and VHDL. It has been evaluated with the Altera Arria 10 FPGA(10AS066N3F40E2SG). Table 4–1 illustrates the FPGA implementation report. The evaluation is separated into two sections, the first subsection demonstrates the general performance and resource utilization shown by the synthesis report in FPGA, while the second subsection

illustrates the performance of the proposed security scheme under timing attacks and SPA.

### 4.3.1 Synthesis results in FPGA

The proposed security scheme was evaluated with a trial synthesis analysis, where an operating frequency of as high as 106.18 MHz was achieved, without violating the clock constraint. However, when considering the circumstances that WBANs would be operating under, an operating frequency of 10 MHz was found to be sufficient. There are two major reasons for this decision. First, compared to BLE [36], WBANs is exchanging data at an even lower rate, since it is unnecessary to request biomedical data from a node at thousands of times per second. For instance, the typical sampling frequency of an ECG sensor is between 50-500 Hz for the original 1000 Hz ECG signal [52], which means the proposed design under operation frequency of 10 MHz could support the communication between the ECG sensors and centralized device easily. As for the body temperature sensors [98] [16], the sampling rate is between few Hz to around 50 Hz, which can also be supported by the proposed design. Second, the latency of the proposed design is close to the connection time of BLE, even when operating at the frequency of 10 MHz, which meets the requirements of the WBANs. Therefore, the operating frequency is determined as 10 MHz for the final synthesis as the typical case, which differs from the trial one when optimizing for power consumption. The resource utilization of the proposed design is demonstrated in terms of adaptive logic modules (ALMs), registers, and memory. The percentage out of the total resources are also listed in Table 4–1.

Table 4–1: Final synthesis results of proposed security scheme

| FPGA | Altera Arria 10 (10AS066N3F40E2SG) |
|---|---|
| ALMs | 7,341/251,680 (2.92%) |
| Registers | 14,743/1,006,720 (1.46%) |
| Memory | 1,007,616/43,642,880 (2.31%) |
| Operating Frequency | 10 MHz |
| Maximum Frequency | 106.18 MHz |
| Power Consumption | 61.86 mW |
| Connection Time | 2.7 ms |

As mentioned before in Section 3, the authentication module and encryption module in the proposed security scheme can operate independently, or together, based on the security level of the communication. In other words, there is only one module operating in some circumstances, resulting in even lower power consumption than the core power shown above. The resource utilization and latency of the authentication module and encryption module are illustrated in Table 4–2. One point that needs to be emphasized is that the latency of the encryption module illustrated in Table 4–2 is the duration of the ECC key generation period of encryption setup phase, as shown in Figure 4–2. This specific latency only occurs once. Afterwards, the latency of the encryption setup phase is the latency of the AES key computation period of each data frame, which is 0.01 ms. Meanwhile, the maximum throughput under the operating frequency of the security scheme is 11.85 Mbps.

Table 4–2: Synthesis report of each module

| Module | ALMs | Registers | Memory | Latency(ms) |
|---|---|---|---|---|
| Authentication Module | 1,529 (0.61%) | 2,048 (0.20%) | 16,384 (0.04%) | 0.95 |
| Encryption Module | 5,812 (2.31%) | 12,695 (1.26%) | 991,232 (2.27%) | 1.75 |

### 4.3.2 Timing attack analysis

Even though the synthesis report of the proposed security scheme in the previous section has illustrated that the proposed design meets power, timing, frequency and other constraints of WBANs, while as a security scheme for WBANs, it is essential to prove its resistance to attacks. As mentioned before, timing attacks and SPA are two of the most common methods for attacks security protocols. Benefit from the natural advantages of Curve25519 provided by Montgomery's Ladder, the execution time of ECC core is fixed, as well as the power consumption. In other words, the proposed security scheme is resistant to timing attacks and SPA theoretically. To prove such the claim, the evaluation of timing attacks and SPA has been done as follows.

For timing attack analysis, 1000 random 32 bytes strings have been selected as the testing values of the public keys in the encryption module, while another 1000 random 32 bytes strings have selected as the testing values of the private keys. Afterwards, 2000 times of executions for different public key and private key random combinations have been performed in FPGA. The execution time has been monitored.

Table 4–3: Execution time for various public and private keys

| Public Keys | Private Keys | Execution Time(ms) |
|---|---|---|
| 1000×32 bytes strings | 1000×32 bytes strings | 1.75 |

The evaluation results illustrated in Table 4–3 proved that for various public keys and private keys, the execution time for a single encryption procedure keeps constant as 1.75 ms for the proposed security scheme for WBANs in the performed FPGA.

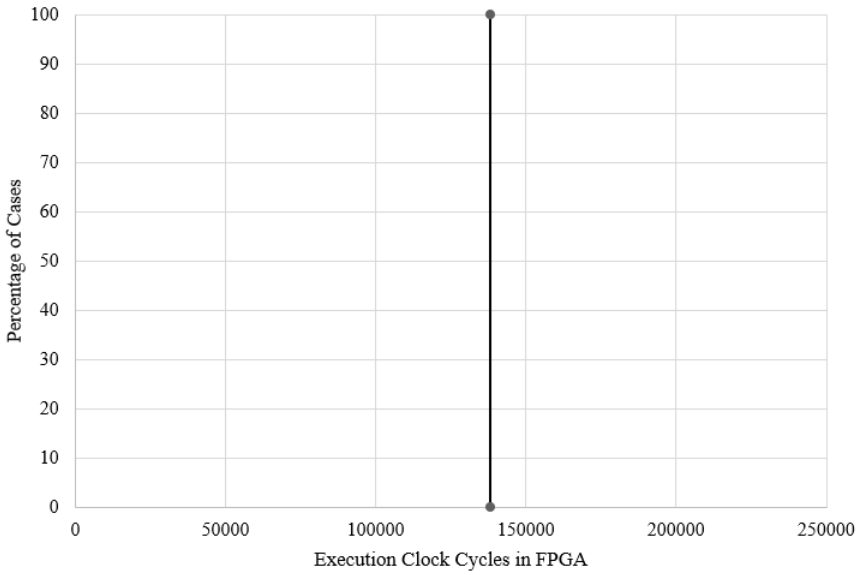



Figure 4–6: Execution clock cycles for different public key in FPGA

Meanwhile, 4–6 demonstrates the execution clock cycles for different 32 bytes public keys, it shows that the execution clock cycles is identical as 138097 clock cycles. In other words, it proved that there are no dependencies between the execution time and the secret stored in the design, and between the power consumption and the secret stored in the design. Therefore, it proved that the proposed security scheme is resistant to timing attacks.

### 4.3.3 Simple power analysis

As mentioned before, as one of the most commonly used methods for attacking, the objective of SPA is to reveal the secret by measuring and inspecting the instantaneous power consumption of a device during the cryptography computing operation depending on the secret. However, the Montgomery's Ladder which has been utilized in the Curve25519 core has the fixed execution procedures theoretically [75],

Table 4–4: Power and energy consumption for various public and private keys

| Public Keys | Private Keys | Power (mW) | Energy Consumption ($\times 10^{-6}$J) |
|---|---|---|---|
| $1000 \times 32$ bytes strings | $1000 \times 32$ bytes strings | 58.42 | 102 |

since it always performs an addition and a doubling for a single stage, which means it is difficult to distinguish combined point double and add operations by different sequence length of patterns in the power trace. It is still necessary to prove that it has identical execution power and energy consumption for different keys for the encryption procedure in hardware.

Similar to timing attack analysis, 2 groups 1000 random 32 bytes strings have been selected as the private key and public key for the test and 2000 times of executions have been performed. The power and energy consumption for every single execution have been recorded.

As is shown in the Table 4–4 and Figure 4–7, for different public and private keys, the power and energy consumption for individual encryption process are fixed to 58.42 mW and $102 \times 10^{-6}$J respectively. It proved that there are no dependencies between the power, energy consumption and the secret stored in the proposed security scheme for WBANs, which means it is resistant to SPA.

## 4.4 ASIC implementation of the proposed security scheme for WBANs

In term of the ASIC implementation of the proposed security scheme for WBANs, it was synthesized by Synopsys using a density and performance optimized high speed library of the SMIC 65nm CMOS technology.

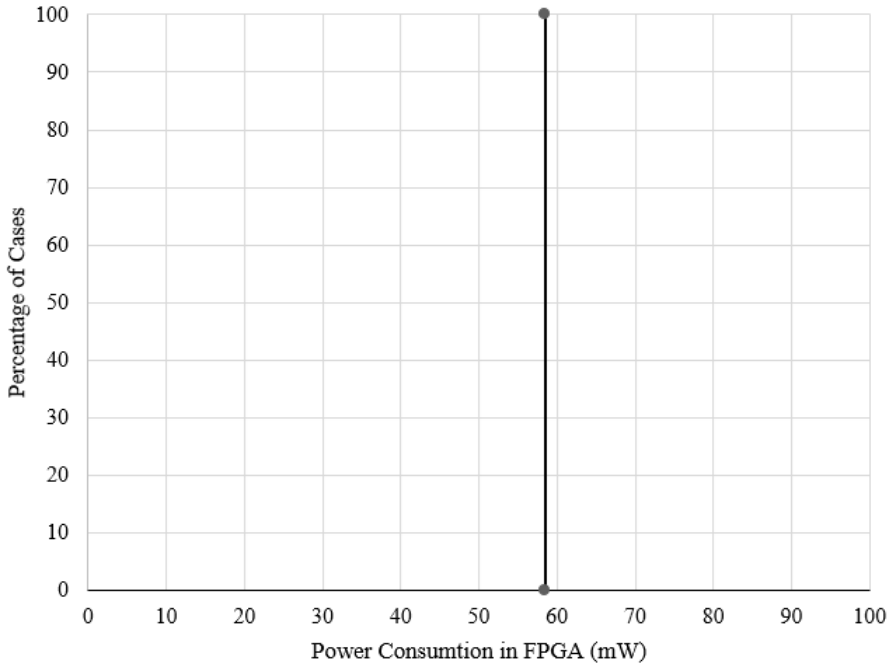



Figure 4–7: Power consumption for various public and private keys

The operating frequency of the proposed security scheme was evaluated with a trial synthesis analysis, where an operating frequency of as high as 500MHz was achieved, without violating the clock constraint. Still, when considering the circumstances that WBANs would be operating under, an operating frequency of 10MHz was found to be sufficient, which meets the requirements of WBANs. Therefore, the operating frequency is determined as 10MHz for the final synthesis which differs from the trial one; the trade-off is it demonstrates a lower power consumption at the same frequency. Figure 4–8 and Table 4–5 illustrate the layout of the final synthesis, and synthesis report, respectively. Even though the operating frequency of the final synthesis is set to be 10MHz, the final proposed circuit can still operate at the frequency of 151MHz without violating the time constraint.

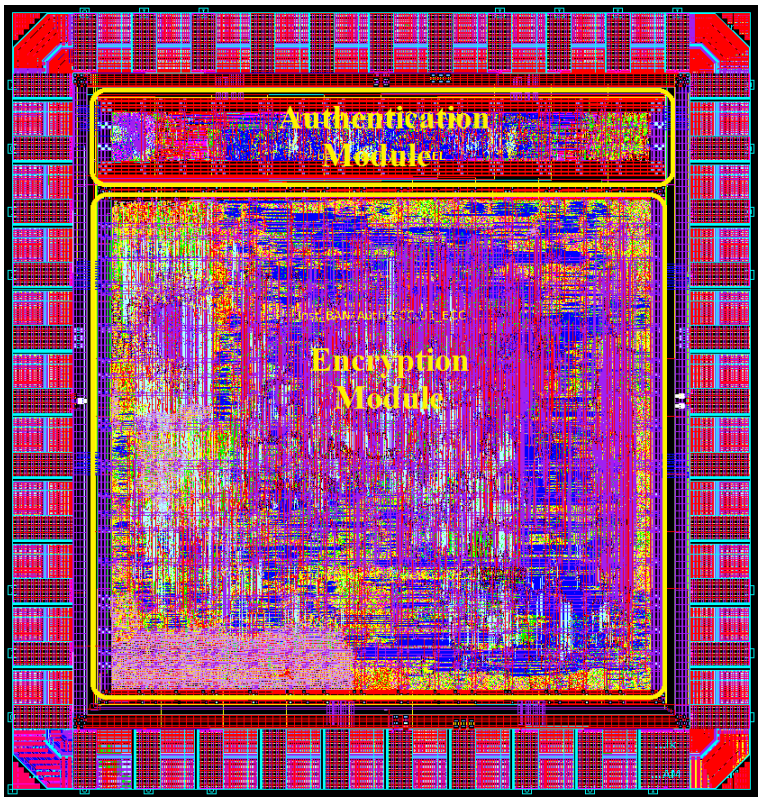



Figure 4–8: Layout of proposed security scheme

Table 4–5: Final synthesis results of proposed ASIC

| Technology | SMIC 65nm CMOS technology |
|---|---|
| Cell Area | 0.72 $mm^2$ |
| Die Area | 1.22 $mm^2$ |
| Logic Gates | 501K |
| Operating Frequency | 10 MHz |
| Maximum Frequency | 151 MHz |
| Core Power | 1.93 mW |
| Latency | 2.7 ms |

As mentioned before, the authentication module and encryption module in the proposed security scheme can operate independently, or together, based on the security level of the communication. In other words, there is only one module operating in some circumstances, resulting in even lower power consumption than the core power shown above. The power consumption, area, and latency of the authentication module and encryption module are illustrated in Table 4–6 respectively. One point needed to be emphasized is that the latency of the encryption module illustrated in Table 4–6 is the duration of the encryption setup phase, as shown in the Figure 4–1. Precisely, this specific latency only occurs once, at the initiation of each communication.

Table 4–6: Power consumption of each block

| Module | Power(mW) | Area($mm^2$) | Latency(ms) |
|---|---|---|---|
| Authentication Module | 0.08 | 0.05 | 0.95 |
| Encryption Module | 1.85 | 0.67 | 1.75 |
| Total | 1.93 | 0.72 | 2.7 |

The final synthesis results illustrate that the proposed ASIC implementation of the security scheme meets the requirements of low power, low latency, and a small area for WBANs. Meanwhile, the operating frequency of the circuit has been optimized to achieve even lower power consumption based on the circumstances that WBANs are applied to, while the latency of the circuit still meets the requirements.

## 4.5 Discussion of the proposed ASIC implementation of security scheme for WBANs

As has been shown previously, the advantages of the proposed security scheme can be summarized as follows. First, the latency of connection is small when compared to BLE. Second, the operating frequency is 10 MHz, which is relatively low, also resulting in low power consumption. Third, in addition to the certificate validation process for authentication purpose, which has been specified and mandated by the standard, a novel challenge-response exchange method involving HMAC-SHA256 is proposed to enhance the security level of authentication. Fourth, the proposed security scheme has relatively low hardware resource utilization. Lastly, the proposed design is implemented in ASIC. Compared to software-based or FPGA-based security schemes, ASIC-based designs have the strength of lower power consumption and higher flexibility in operating frequency.

However, the proposed security scheme also has limitations. Since it is implemented in hardware, additional corresponding integrated circuits have to be installed, on both the hub side and node side, when applying the security scheme for the WBANs. This increases the difficulty of the application when compared to software-based designs. Meanwhile, the cost of hardware implementations is also higher than software-based security schemes.

## 4.6 Using the characteristic value of the body channel for encryption of WBANs

As mentioned, communication in WBANs requires high-level security protection since WBANs are transmitting the most critical and private biomedical information between the hubs and nodes. At the same time, WBAN systems especially the nodes

have an extremely limited power supply. However, common encryption methods found in computer networks are not ideal due to complex algorithms and high-power consumption. Therefore, a new encryption method based on the human body channel has been proposed in this section. This new encryption method has the advantages of low-power, dynamic updating, rapid operation, and easy implementation, which is suitable for WBAN systems.

In terms of other encryption methods for WBAN system other than the ECC encryption specified in IEEE 802.15.6 standard, [18] puts forward a multi-path reinforcement method, whereas [72] and [116] generate the keys according to the periodicity of physiological signs information. However, the requirement of lower power consumption in WBANs needs to be considered. In this section, a method is proposed in which keys are based on the WBANs channel characteristics.

### 4.6.1 Human body channel model

The human body channel model needs to be established since the proposed encryption method is based on the characteristic value of the WBANs channel. Being different from other communication channels, the WBANs channel is dynamic and depends on the human body. Establishing the human body model and calculating the parameters of the WBANs channel is, therefore, necessary for exploring the channel. To establish the three-dimensional body channel model, the VariPose simulation software is used. VariPose is a software that models the human body in various postures, and it can be used to obtain different positions of the human body channel through the method of the human grid. Different kinds of dielectric constant and conductivity of human tissue are used to simulate the human grid and build the

channel model. The established channel model is imported into the XFdtd software to simulate the bio-electromagnetic field, which utilizes the Finite-Difference Time-Domain (FDTD) method.

### 4.6.2 Software parameter configuration

The corresponding path loss value in the WBAN systems is calculated with the XFDTD software. The path loss discussed is at 2.4 GHz, and a half-wave dipole antenna is simulating the transceiver, which is placed 2 mm apart from the human skin. The impedance is set to 50 Ω, and the incident wavelength is $\alpha$, thus, the length of the antenna $L$ is $\frac{\alpha}{2}$ and the radius of the antenna $\gamma$ is $\frac{\alpha}{200}$; $L$=62 mm and $\gamma$=0.62 mm at 2.4 GHz.

**Channel path loss**

With the aid of the XFDTD software and the human body channel model, the effect the distance between transmitters and receivers has on the channel characteristics can be observed. The transmitter antenna is fixed on the right-hand wrist, the receiver antenna is not fixed, and the distance of the transmitter and receiver is adjusted by changing the position of the receiver antenna.

The path loss is defined as the signal power ratio of the channel output over the channel input and is represented as $S_{21}$. This electromagnetic wave attenuation is the characteristic value of the WBANs channel. Table 4–7 shows the $S_{21}$ values of human body channel at different distances between the antennas, with the negative sign indicating a loss.

Table 4–7: $S_{21}$ values of human body channel

| d(mm) | $S_{21}$ | d(mm) | $S_{21}$ |
|---|---|---|---|
| 25 | -28.74 | 300 | -63.97 |
| 50 | -30.12 | 325 | -65.38 |
| 75 | -32.47 | 350 | -66.04 |
| 100 | -36.1 | 375 | -67.16 |
| 125 | -37.61 | 400 | -68.92 |
| 150 | -44.86 | 425 | -69.34 |
| 175 | -50.02 | 450 | -69.87 |
| 200 | -55.43 | 475 | -70.16 |
| 225 | -56.53 | 500 | -70.69 |
| 250 | -58.97 | 525 | -71.25 |
| 275 | -61.25 | - | - |

**Channel simulations**

To simulate the human body channel, 9 snapshots are extracted from a human walk, as shown in Figure 4–9. The 62 mm length half-wave dipole antennas are simulated, with the transceiver antennas on the right waist and the left ankle. As before, the antennas are placed 2 mm apart from the human skin and the transmitting frequency is 2.4 GHz. The path loss values are calculated in each snapshot by the simulation.

Table 4–8: Human body channel path loss of each snapshot at 2.4GHz

| Snapshot | $S_{21}(dB)$ | Snapshot | $S_{21}(dB)$ |
|---|---|---|---|
| 1 | -66.275 | 6 | -65.623 |
| 2 | -70.146 | 7 | -68.546 |
| 3 | -72.068 | 8 | -72.429 |
| 4 | -65.567 | 9 | -72.679 |
| 5 | -62.246 | - | - |

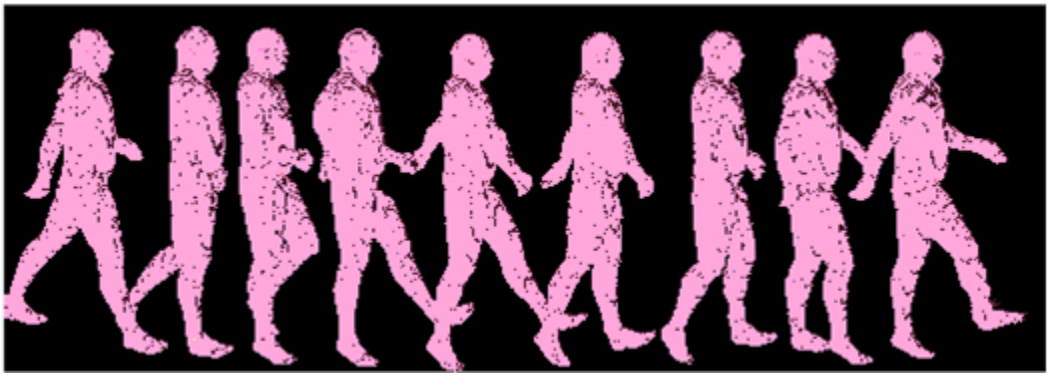


Figure 4–9: The nine snapshots of human walk

As shown in Table 4–8, when the human posture changes so do the communication link between the right waist and the left ankle, resulting in a path loss change in each snapshot. The average fluctuation is 2.89 dB, the maximum path loss value of 72.679dB appears in the 9th snapshot, and the minimum path loss value of 62.246 dB appears in the 5th snapshot (in this snapshot, the left foot of the human body is straight forward, and the right foot is backward, and thus the antennas are unobscured by the human body). The difference between the maximum and the minimum path loss is 10.43 dB.

### 4.6.3 Proposed encryption enhancement method

To reduce power consumption in the WBAN systems, the computation during the data encryption is minimized. As illustrated in Figure 4–10, the encryption process is: first, the transmitting power information of the sensor node and the leading sequence is transmitted from the node during the initialization, and the sensor node does not perform any computations. Second, the coordinating node on the receiving end computes the characteristic values of $S_{21}$ based on the transmitting power information of the node, the leading sequence, and its receiving power. It

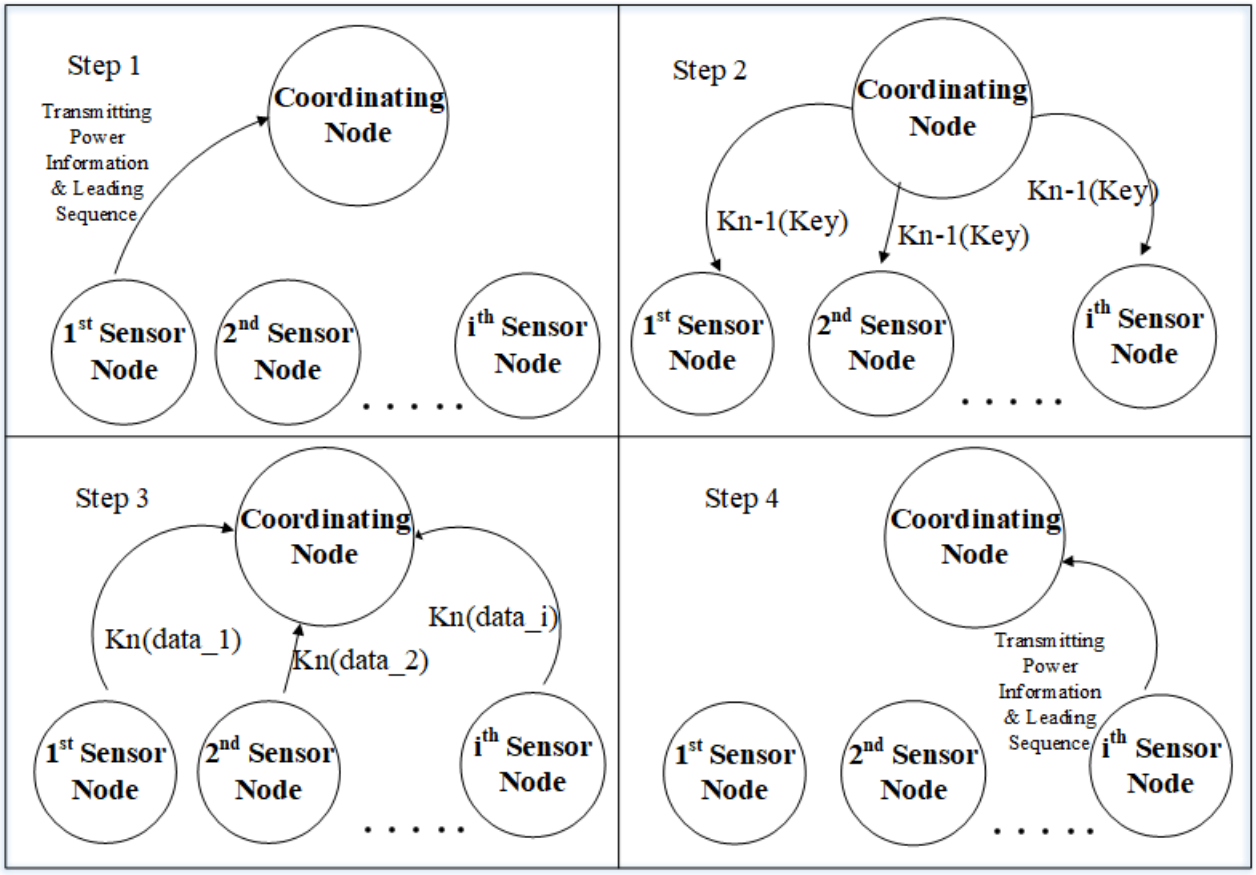



Figure 4–10: Proposed dynamic encryption sequence based on the characteristic value of the body channel

then generates a key based with the Linear Feedback Shift Register (LFSR) circuit, encrypts the current key with the key from the previous sequence, and broadcasts them. Third, the sensor node encrypts the WBANs data according to the current key received from the coordinating node. Last, the system will randomly select a sensor node to send the leading sequence to the coordinating node over time, and the coordinating node will re-compute the key based on the transmitting power and receiving power. Therefore, the encryption method calculates the characteristic values to form the key in the coordinating node. The other sensor nodes do not have to perform any heavy computational tasks, which effectively reduces the power consumption of the whole WBAN system. Moreover, if an eavesdropper somehow gains access to the key at a point, it can only gain access to a small part of information due to the key changing shortly after.

**Key generation**

After detecting the path loss value for a short period of time $t$, which is no more than a few seconds, the characteristic value $\lambda$ can be calculated as:

$$\lambda = \frac{\sum_{i=1}^{n} S_{21}^{i}}{n} \tag{4.26}$$

where $S_{21}^{i}$ is the amplitude of the $i^{th}$ $S_{21}$ of the sensor nodes and coordinating node within the short period of time $t$. The channel path loss has a significant difference on different individuals, while, even for a single individual the path loss will vary over time. Therefore, the characteristic value of $\lambda$ is dynamically updated, and the key is refreshed based on $\lambda$. Additionally, in the actual applications of WBAN systems, $S_{21}$ is the ratio of the receiving power over the transmitting power. The receiving

power and the transmitting power are easy to obtain from RF (radio frequency) chips without any additional costs, therefore, this method is conducive to low power implementation of the sensor nodes in WBANs. The characteristic value is quantified as the initial key for the LFSR with $N$-order to generate the stream key. The keystream broadcasts to the nodes in the WBAN system, and the nodes use the key to decrypt the data. The encryption method will re-generate the key, and the above steps are repeated at regular time intervals of $T$ (where $T >> t$).

**Method of LFSR circuit encryption**

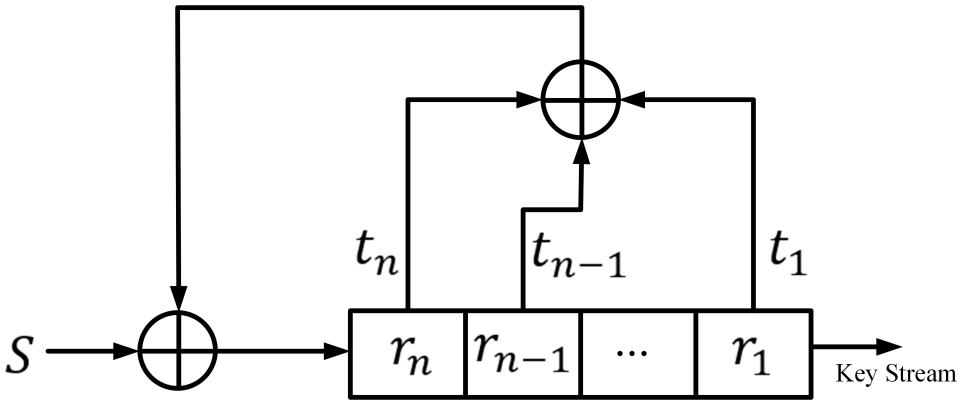



Figure 4–11: The LFSR based private key generator

Different from software encryption, Circuit level encryption has the advantages of lower consumption, Higher security, and stability. Basing on the channel characteristic values, this design adopts the LFSR circuit to produce the stream cipher. The n-level LFSR consists of the shift register $R = (r_n, r_{n-1}, \ldots, r_1)$, the tap sequence $T = (t_n, t_{n-1}, \ldots, t_1)$ and the enter digital signature S. As shown in Figure 4–12, when generating a new key, one of bits in digital signature and the feedback bit form a new bit through a operation, then the new bit would insert the shift

register, and the right side output a bit at the same time, the other bits moves one bit to the right in turn. The structure of the key generator could output the self-circulation keystream, meanwhile, the circuit construction of the key generator is relatively easy and some logic gate would provide high security. But if the eavesdroppers master a certain number of corresponding plaintext and ciphertext, the tap sequence would be deduced and then crack the encryption system. Therefore, the structure needs to be optimized. This proposed work adopts a 16-order linear feedback shift register to extend the period, and its maximum value is $2^{16}$. In addition, the dynamic key update is essential, because the key is refreshed every T seconds leading to a lower probability of cracking. Compared to using software encryption

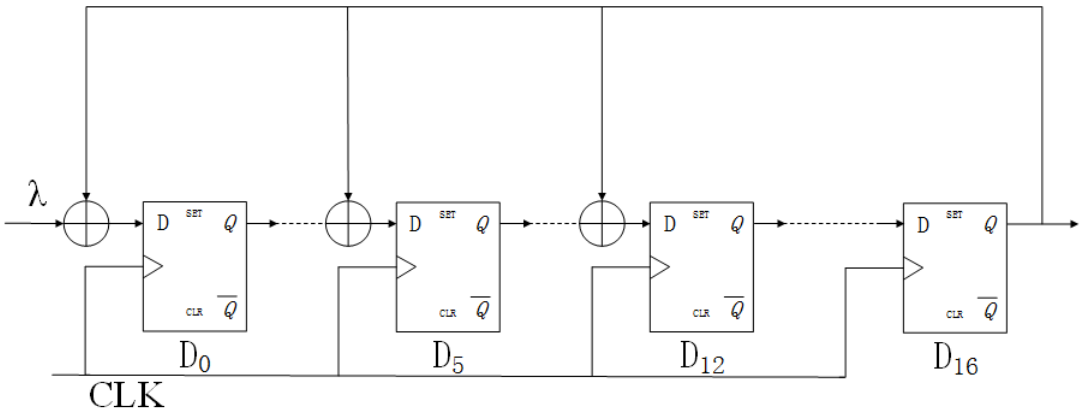


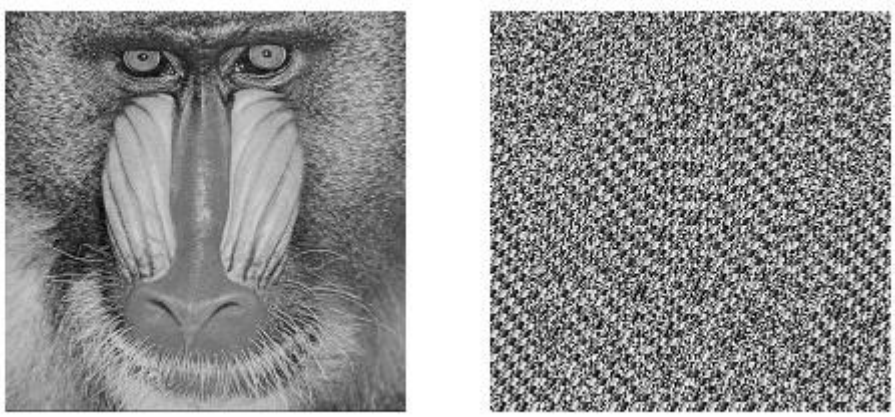

Figure 4–12: 16-order LFSR

algorithm alone, the LFSR circuit has the fast conversion speed [117] and simple hardware implementation. Therefore, a 16-order LFSR circuit is used to encrypt the WBANs plaintext. As shown in Figure 4–12, the polynomial of 16-order LFSR is $F(X) = X^{16} + X^{12} + X^5 + 1$. Moreover, the dynamical update of the key based

on the $S_{21}$ value at regular time intervals $T$ can ensure real-time encryption, which significantly reduces the possibility of an attack.

### 4.6.4 Experiment results and analysis of encryption

Figure 4–13 shows the figure result of the encryption proposed, using an 8-bit grayscale image of a baboon. In this experiment, the pixel intensity probability



(a) Original Image (b) Encrypted Image

Figure 4–13: Encryption results of baboon image

distribution was investigated. Figure 4–14 shows the pixel intensity probability distribution histogram of the plaintext and ciphertext images of the baboon. The plaintext image of Figure 4–14 (a) shows that the pixel intensity distribution has certain specific regularity. However, as shown in Figure 4–14 (b), the distribution of the pixel intensity in the encrypted image is evenly balanced. The proposed encryption method disrupted the probability distribution of the pixel intensity found in the original image. This result indicates that the encryption method based on the keystream would be able to effectively resist statistical attacks.

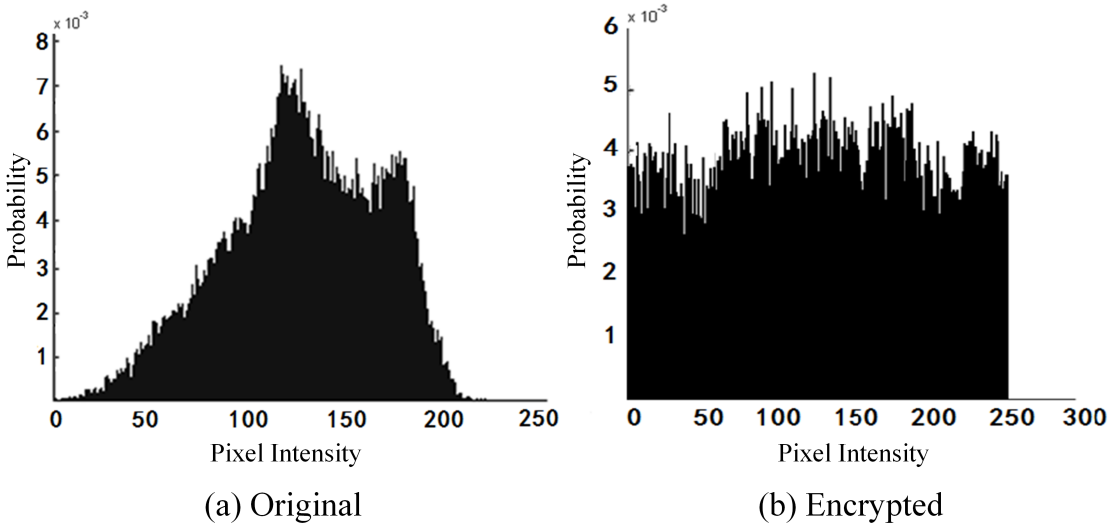
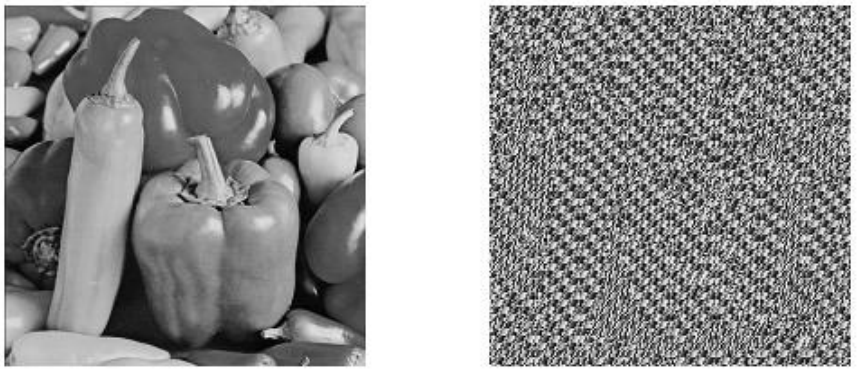



Figure 4–14: The original and encrypted statistical histograms

The encryption algorithm needs to have a strong sensitivity, such that a small change of the key will result in a decryption plaintext that is totally different from the original plaintext. For this experiment, the WBANs channel characteristics are used to compute the initial key and then used to encrypt an image with peppers. The encrypted image is then decrypted with a key that has a slight difference; one bit of the initial key is changed, more specifically, one bit of the initial value of the 16-bit shift register is randomly selected and inverted. This initial key is then used to generate the key stream. Figure 4–15 (a) shows the decrypted image when the correct key was used, and Figure 4–15 (b) shows the decrypted image when the wrong key, that is, the key with the difference, was used. As shown in the figures, even a small change in the key will result in incorrect decryption. Paper [117] shows that this algorithm demonstrates excellent performance to differential attacks. Therefore, the NPCR (Number of Pixels Change Rate) and the UACI (Unified Average Changing



(a) Decryption using the Correct Key (b) Decryption using the Wrong Key

Figure 4–15: Test result: the sensitivity of the algorithm

Intensity) are being used to measure the sensitivity of the encryption algorithm. In this sensitivity measurement, two similar plaintext images were used, in which one pixel, $(i, j)$, is different. After the key stream encryption, the intensities of the $(i, j)$ pixel in the two images are $C_1(i, j)$ and $C_2(i, j)$, respectively. It is defined that if $C_1(i, j) = C_2(i, j)$, $D(i, j) = 0$, and if $C_1(i, j) \neq C_2(i, j)$, then $D(i, j) = 1$. The formulas of NPCR and UACI are:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\% \tag{4.27}$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\mid c_1(i, j) - c_2(i, j) \mid}{255} \times 100\% \tag{4.28}$$

The ideal values of NPCR and UACI are:

$$NPCR_E = (1 - 2^{-n}) \times 100\% \tag{4.29}$$

$$UACI_E = \frac{1}{2^{2n}} \frac{\sum_{i=1}^{2^n - 1} i(i + 1)}{2^n - 1} \times 100\% \tag{4.30}$$

where $M$ and $N$ represent the row number and the column number of the image pixels respectively. $D$ is 0 or 1, as defined above, and the experiment images are 8-bit grayscale, thus $n = 8$ in the formulas (4) and (5). The ideal values of NPCR and UACI can be calculated as 99.61% and 33.46% respectively. This experiment utilizes the image with the baboon to test the NPCR and UACI, by randomly selecting one pixel in the image and inverting its lowest bit to generate another image. The calculated experiment values of NPCR and UACI are 99.46% and 49.0138% respectively. When compared with the ideal values, it can be seen that the experiment NPCR values are close to the ideal values, but the experiment UACI values are quite different from the ideal values. This is because the encryption method is lightweight, and it can ensure the pixel change rate but not the pixel change strength.

### 4.6.5 Discussion of the proposed encryption method using the characteristic value of the body channel

In this section, a new encryption method is proposed which uses the channel characteristic values as the initial key, and introduces the LFSR circuit to generate key streams and encrypt the WBANs data. The new method has the advantages of dynamic keys, low power consumption, rapid operation, and easy implementation. Experimental results show that the encryption method can be helpful for designing low-power WBAN systems, which provides theoretical support and engineering implementation.

In future, more research attention will be invested in the hardware implementation of the proposed encryption method using the characteristic value of the body channel, and the cooperation between the proposed encryption method and other security designs in the WBAN systems.

## 4.7 Summary of the chapter

In this chapter, a security scheme for WBAN systems has been proposed based on the specifications of IEEE 802.15.6. Initially, we include the background and previously published work related to security of WBAN systems. Afterwards, the proposed security scheme is described as the algorithm level and implemented in FPGA to verify the design. Then, the proposed security scheme is implemented in ASIC and synthesized by SMIC 65 nm CMOS technology. The final synthesis results illustrate that the proposed security scheme meets the requirements of low power, small latency, and small hardware cost for WBAN systems. Meanwhile, the operating frequency of the design has been optimized to achieve an even lower power consumption than required in the circumstances that WBANs are applied to, while the latency of the circuit still meets the requirements. Finally, to further decrease the power consumption of WBAN systems, the author presents an encryption method using the characteristic value of the body channel for WBAN systems, which has lower complexity and power consumption than the traditional encryption methods.

# CHAPTER 5
# A Blockchain-Based eHealthcare System Interoperating with WBANs

Due to the increasing population of the elderly and patients with chronic diseases, more and more individuals are suffering from the limited service capabilities of the traditional medical systems. Benefiting from the rapid development of biomedical sensors, Internet of Things, and modern communication and network technologies, eHealthcare systems start appearing in the medical services, especially for the remote physical condition monitoring which improves the efficiency of the traditional medical systems. In this chapter, a blockchain-based eHealthcare system interoperating with WBANs has been proposed, which utilizes the WBANs as the communication protocol for the networks around the human body of the patients and blockchain technology as the data transmitting and storage method. The evaluation results show that the proposed system has the advantages of low hardware resources utilization, high-security protection level, and stable performance.

## 5.1 Introduction of the chapter

The number of patients with chronic diseases in the world has increased from 118 million to 149 million in the past 25 years, while the number will rise to 171 million in the next 10 years [1]. However, inefficient conventional medical and healthcare systems cannot provide timely and efficient medical services to the public. For instance, based on the report by the Fraser Institute [10], the average waiting time for consulting medical professionals was 21.2 weeks in 2017 in Canada. In other words,

the current and future patients need to wait for around 5 months in the queues before consulting the medical doctors about their physical conditions. To shorten the waiting time for consulting medical professionals, some countries with a huge population such as China started to adopt the triage-type hierarchical diagnosis and treatment based on the conditions of the patients[44]. Even though it helped improve the efficiency of traditional medical systems, there is still a huge demand for efficient, economical, and secure healthcare systems, which can not only monitor the physical conditions of the patients but also store the data and give feedback to the patients under protection if necessary. Fortunately, with the rapid development of modern technology, eHealthcare systems provide the possibility to address such a demand. Precisely, by utilizing modern biomedical sensors, various types of networks, and cloud storage, an eHealthcare system can support all stages of care for the patients including prevention, diagnosis, treatment, and follow up remotely [41] as illustrated in Figure 1–1.

Generally, an eHealthcare system has two types of communication protocols. One is the network around the human skin surface which supports the communication around the human body between the biomedical sensors and the centralized devices at the front-end, while the other one is the pervasive social network such as the Internet which supports the communication between the operation exchange center and other participants in the back-end. In term of the communication protocol around the human skin surface, even though Bluetooth and Zigbee have been widely utilized in eHealthcare systems, the drawbacks of them are obvious. Since none of Bluetooth or Zigbee is dedicated to eHealthcare data transmission, the frequency,

data rate, power consumption, and security schemes are not suitable for eHealthcare circumstances [65]. In 2012, a communication protocol standard of WBANs, which is IEEE 802.15.6, was released. The standard specifies the details regarding the communication according to the characteristics of the data that needs to be transmitted between the biomedical sensors and centralized devices. To be more precise, compared to Bluetooth and Zigbee, WBANs are more sensitive to the power consumption due to the power supply constraints [51] while it has lower requirements for the frequency, data rate, and bandwidth since the data collected by the sensors is relatively simple and the transmission period could be much longer. Meanwhile, the standard of IEEE 802.15.6 also specifies a lightweight security scheme consisting of authentication and encryption, which is dedicated to WBANs [79] [101]. In addition, a data transmitting mechanism has been proposed for WBAN systems which improves the data transmission efficiency[3].

In recent years, the blockchain technology has attracted huge academic and industrial research attention due to its characteristics of consensus and decentralization [54] [85]. By utilizing blockchains, different peers in the system can achieve the same functionality with the same amount of certainty without having a central authority [73] [25] [24]. Therefore, a blockchain-based eHealthcare system interoperating with WBANs is proposed in this chapter. WBANs can be found in the front-end of the system, where it interconnects sensor nodes together, which in turn interact with a blockchain network found in the back-end. The front-end is also comprised of the users participating in the system. Benefiting from the combination of WBANs and blockchain technologies, the advantages of the proposed system are as follows. First,

the power consumption is relatively low in the local networks around the human skin surface of the patients. Second, data from different participants in the system are trustworthy. Third, computation, analysis, and data storage are decentralized without having a central authority in the back-end, which ensures the security environment of network and the privacy of the data while it decreases the cost of establishing the system. Further, the immutability and non-repudiation properties of the blockchain back-end offer powerful anti-tampering logging and auditing. However, there are three main disadvantages of blockchain technology [69]. First, due to the complexity of the algorithms of the blockchain, it requires higher computing ability and power consumption from each node in the blockchain network than other conventional systems. Second, implementing a blockchain-based data transmitting and storage system is more complicated than traditional information systems. It requires engineers with higher professional skills in blockchain to implement, optimize, and maintain the system which could increase its cost. Third, due to differences between the blockchain platforms (such as Hyperledger, Ethereum, etc.), different blockchain implementations will be incompatible with each other. The blockchain, by definition, is based on certain principles such as cryptography hashing, certificates, proof of work, and so on, however, there is no standard mandating consistency between different platforms.

The motivations of the research are demonstrated as follows. First, it has been demonstrated that the blockchain technology can ensure the security environment of the networks when applying into finance, and insurance fields due to the features of decentralized storage and achieving consensus [107]. Meanwhile, the security of

eHealthcare system could also benefit from those features of the blockchain technology. Moreover, as the most fundamental element of the eHealthcare system, WBANs supports the communication between biomedical sensors attached or implanted in the human body with the centralized devices of the patients, which is protected by its own security scheme. The interoperation between the security scheme of WBANs and the security specifications of the blockchain-based eHealthcare system could be a challenge when they are working together with each other to ensure the security of the whole system. Few published works can be found regarding the security issues of interoperation between WBANs and eHealthcare systems [11] [81]. However, they only proposed the security scheme and privacy protection solution for non-blockchain eHealthcare systems. In this chapter, a blockchain-based eHealthcare system interoperating with WBANs has been proposed, which is bringing together the advantages of both technologies in a compatible and meaningful way.

The chapter is organized as follows. The background and related work are presented in Section 5.2. Afterwards, in Section 5.3, the functionality description and system architecture of the proposed blockchain-based eHealthcare system interoperating with WBANs are demonstrated. Moreover, the implementation and evaluation of the proposed system are shown in Section 5.4. Finally, the last section concludes the chapter and lists potential ideas for future extensions of this work.

## 5.2 Background and related work

### 5.2.1 WBANs basics

In 2012, the IEEE 802.15.6 standard for WBANs was released, which specifies the communication parameters (frequency, data rate, etc.) based on the characteristics of the data transmission in WBANs. WBANs provides a communication protocol dedicated to the communication between the biomedical sensors and centralized devices around the human skin surface since it meets the requirements for efficient, economical, and uninterrupted health condition monitoring. Compared to conventional wireless communication protocols such as Bluetooth and Zigbee, the communication range, transmission speed, and bandwidth of WBANs are relatively small since the nodes in WBANs are extremely sensitive to the power consumption due to the battery supply constraints, especially for implanted devices [65]. Meanwhile, the IEEE 802.15.6 standard also specifies a unique lightweight security scheme consisting of authentication and encryption which provides enough data protection while the power consumption is also acceptable [102].

One of the most critical advantages that WBANs have compared to other wireless communication protocols is ultra-low power consumption at different data rates. For instance, when the data rate is 1Mbps, the power consumption that WBANs can achieve is as low as 0.1 mW to 8 mW, while the power consumption of Bluetooth is between 8 mW to 100 mW. In addition, when the data rate is 100 kbps, the power consumption of WBANs is between 0.03 mW to 8mW while it is 5 mW to 50 mW for Zigbee [65]. Meanwhile, the wireless communication in WBANs has less interference, since it supports a large range of transmission frequencies from 400 MHz to 5 GHz,

while Zigbee and Bluetooth are all working at 2.4 GHz [65]. Furthermore, the IEEE 802.15.6 standard specifies a unique security protocol to protect the communication in WBANs [81].

In terms of the security specifications of WBANs, there are three security levels specified in the communication of WBANs, which are Level 0, Level 1, and Level 2 respectively [81]. The security level of communication in WBANs is determined by the information contained in the communication. The unsecured communication identified as security Level 0. It only contains non-confidential information such as timestamps. In these cases, neither authentication nor encryption is required. The communication specified as security Level 1 contains private but not critical information such as name, age, gender, and locations, which shall not be accessed by someone does not has the authority. Therefore, authentication is necessary for this communication. In terms of Level 2, the communication contains most confidential information including biomedical data collected from the patients, the feedback from the hospitals and doctors, the parameters for the insulin pump, and so on. This data has a direct relationship with the physical conditions of the patients and intruding into the communication could cause fatal health issues. Therefore, for the communication specified as security Level 2, both authentication and encryption are required. In terms of the methods used for authentication and encryption, the IEEE 802.15.6 standard has specified the validation of certificates as the method for authentication, and ECC as the way to generate the key for AES, which is the encryption method to be used [42]. Meanwhile, the standard also leaves some room for the engineers

to improve the security performance of the WBAN systems regarding the detailed implementations of the security scheme of WBANs.

### 5.2.2 Blockchain basics

In 2008, blockchain was invented by Satoshi Nakamoto [82] to serve as the public transaction ledger of the bitcoin, which addressed the issue of double spending for digital currency without a trusted authority. Afterwards, the blockchain technology has been applied to various areas such as finance, insurance, as well as healthcare systems [68].

Generally speaking, blockchain is a technology which can build a distributed database consisting of a list of blocks. Meanwhile, the blocks in the database are connected with each other, and every node in the blockchain can not only generate the blocks but also store them. In terms of the data structure of the block, it contains the timestamp of its generation, the hash of the previous block, and the transaction data [24]. Therefore, different nodes in the blockchain can achieve consensus without a trusted authority, which provides better privacy protection than conventional centralized network technologies[25] [37].

### 5.2.3 Related work

Since the personal data collected by biomedical sensors in WBANs and other health-related data in the eHealthcare system, including blood pressure, glucose level, parameters for insulin pump, parameters for pacemakers, and so on, are extremely critical and hacking into the eHealthcare system could cause fatal health issues [120], the blockchain technology provides a potential solution of distributed data management for eHealthcare systems.

There are few publications discussing the possibility of applying the blockchain technology in healthcare applications; in 2016, [114] proposed a secure system for pervasive social network based healthcare, while the authors focused more on the network side instead of the realistic medical application circumstances. In the article [50], the authors discussed the utilization of blockchain distributed ledger technologies for biomedical and healthcare applications. The benefits of blockchain for biomedical and healthcare applications were illustrated in [50], while the system architecture and detailed implementation were not given. Meanwhile, a decentralized personal data management system using blockchain was proposed in 2015 [122], this research focused on the privacy protection and data management of personal data, while the system architecture of the eHealthcare system was not given.

## 5.3 Proposed blockchain-Based eHealthcare system interoperating with WBANs

### 5.3.1 System architecture

Figure 5–1 illustrates the architecture of the proposed blockchain-based eHealthcare system. In terms of the roles in the proposed system, there are patients, medical doctors, medical center(s), insurance providers, medicament suppliers (including common pharmacies) and emergency services. The detailed functionality and operations of each role are specified by smart contracts between the parties, and its overall operation is demonstrated in the following subsections. The data transmission between the sensors and centralized devices around the patients is supported by WBANs in the front-end, while the blockchain-based data transmission and storage system apply to all the roles in the proposed system.

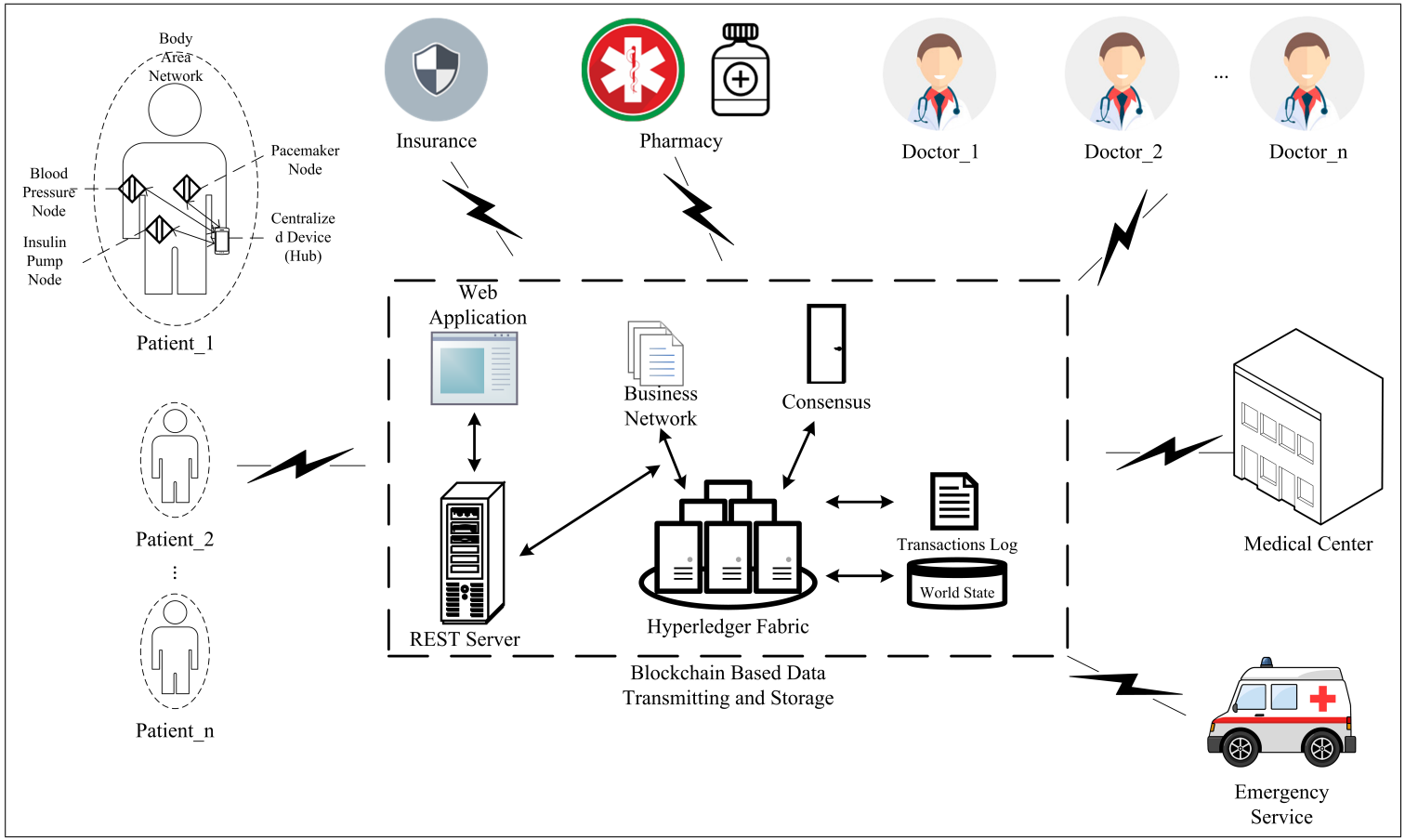



Figure 5–1: Architecture of proposed system

### 5.3.2 Roles in the proposed Blockchain-Based eHealthcare system

As mentioned before, there are six roles in the proposed system which are patients, doctors, medical center(s), emergency services, insurance providers, and medicament suppliers, as shown in Figure 5–1.

As the most fundamental part of an eHealthcare system, patients need to transmit the biomedical data collected from the sensors to the centralized devices for every period $t$ which is specified by the stack of the centralized devices. Meanwhile, centralized devices give the latest instructions to the sensors. The communication protocol in this scenario is WBANs which is dedicated to the communication between the sensors and the centralized devices. Afterwards, the centralized devices generate the information structure which contains the patients' ID, patients name, corresponding medical doctor, time, and location information, then submit a transaction to the blockchain network to update the physical data of the patients.

In terms of medical professionals, every individual physician only has access to the physical record of the patients who have been assigned to them. Meanwhile, doctors could also give medical instructions to the patients by submitting transactions to update the medical instructions. The structure, in this case, contains the corresponding patient, the ID of the doctor, medical instructions, and time. The patients who are assigned to the specific doctor grant access to their own medical instructions.

Medical centers and emergency services are two parts that interoperate with each other closely in the proposed eHealthcare system. Medical centers have the highest authority to access all of the medical data in the blockchain. There are two

functionalities for the medical centers, one is assigning different doctors to various patients, while the other is to assign the emergency services to specific patients based on the physical condition of the patients, which are collected by the WBANs around the patients. Once the emergency service has been assigned to a patient, it will have access to all the medical and physical record related to the specific patient until the emergency service is terminated.

For patients that need renewable supplies of medicaments, the contract between the patient, insurance providers and medicament suppliers (both the original producers and distributors such as pharmacies) specify the exact condition under which the medicament renewal is safe to supply, as well as when all the payments are received. The feedback information on the quantities of medicaments is also made available (under all privacy protection mechanisms) to physicians and medicament makers, such that the dosing of the medicaments can be optimized and also personalized for a given patient.

### 5.3.3 WBANs in integrated the eHealthcare system

WBAN is a communication protocol which is dedicated to the short-range communication between sensors and centralized devices, which is regulated by the IEEE 802.15.6 standard. In the scenarios of the proposed eHealthcare system, WBANs have been utilized as the communication solution for the data transmission between the sensors and centralized devices around the patients. As specified by the standard, the transceivers of WBANs consist of BCH encoder, spreader, bitwise interleaver, scrambler, symbol mapper, RF front end, and corresponding inverse operation modules[101] as illustrated in the Figure 5–2. Benefitting from the nature of

WBANs [65], the power consumption for the patients' side has been reduced dramatically compared to Bluetooth. The detailed implementation and evaluation of the WBANs in the proposed system are demonstrated in Sections 4 and 5.

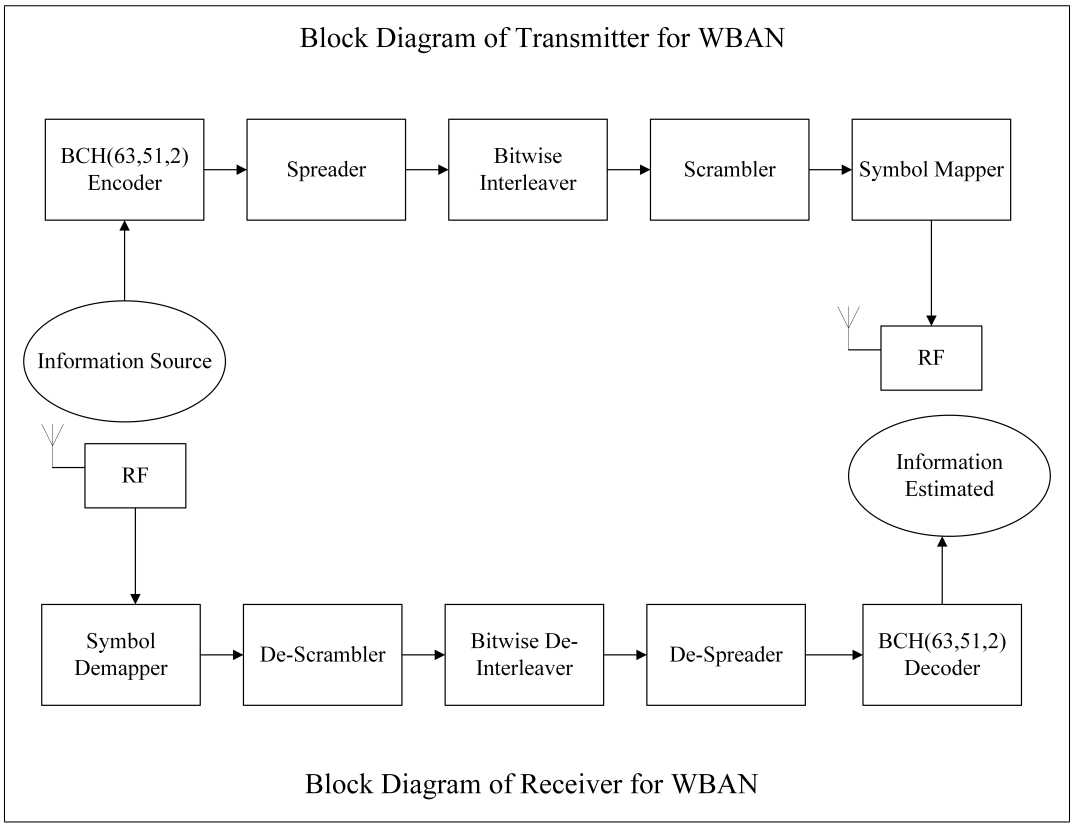



Figure 5–2: Block diagram of transceiver for WBANs

### 5.3.4 Blockchain-based data transmitting and storage in the proposed eHealthcare system

In a conventional medical system, all the data is stored in a central database. Based on the roles in the medical system, different users shall have various permissions to access different types of data. For instance, medical doctors shall have access to all the data belonging to their corresponding patients, while an ambulance

shall have access to the location and the historical medical record of a patient who has been assigned to rescue. However, the drawbacks are obvious: once the central database has been attacked or the data in a central database has tampered, all the participants of the system will be impacted. In a blockchain-based system, the ledger is append-only and distributed. There is no single point of failure, and tampering is not feasible. Altering data requires submitting a correction transaction which is subject to the nonrepudiation properties of the blockchain, that is, every transaction is cryptographically signed and secure. Further, the transaction needs to be endorsed by the relevant parties. The combination of an append-only ledger requiring cryptographically signed transactions achieves powerful, immutable logging and auditing. The endorsement also ensures the transactions will only be accepted if they meet the endorsement policies specified in the medical system. Last but not least, the privacy of data and access to it can be enforced through access control rules.

The blockchain-based data transmitting and storage module is composed of several sub-modules, each of which has a different function.

Hyperledger Fabric is the core of the blockchain module, it is a Distributed Ledger Technology (DLT) platform designed for the enterprise. In an enterprise use case, several things need to be considered. For instance, the participants need to have identities; the networks need to be permissioned; and the transactions need to be private and confidential. Hyperledger Fabric was designed with these things in mind. It is configurable and supports modular consensus protocols, which need not require a cryptocurrency to incentivize mining or smart contract execution. This

reduces the risk of attacks and makes the computational power required compared to that of any other distributed system.

Hyperledger Fabric relies on two components, the transaction log, and the world state, to make a ledger. Concisely, the world state is the current state of the ledger, that is, a Key-Value Pair (KVP) database showing the state of the system at any given moment. The transaction log, on the other hand, also called blockchain, is the log of all transactions, consisting of all the changes that have been made to the world state that result in the current state of it. Following the transaction log can recreate the current world state. A good analogy for the world state and transaction log is the current balance and history of transactions in a banking account. It is easy to understand that following the history from the creation of the banking account will result in the current balance. The ledger is replicated on every peer.

As discussed, Hyperledger Fabric does not feature or incentivize mining. In fact, it does not use computationally expensive consensus algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) varieties. Instead, various consensus algorithms, for example, Byzantine or crash fault tolerant, can be implemented. The method that they achieved consensus is by ensuring the participants are identified and authenticated to submit transactions. In other words, the network is permissioned and participants trust each other, albeit not to an unconditional extent.

Hyperledger Fabric achieves consensus by ensuring that all transactions taking place are confirmed to be correct and execute in order. A transaction flow will be presented here. The transaction will be proposed at first by a peer, and then sent to endorsing peers as specified by the endorsement policies. The transaction will then be

simulated by the endorsing peers that will validate and vote for the transaction. The results are then broadcast to the ordering service, which will order the transactions into lists of records called blocks, before sending them to the peers, where they are finalized in each peer's copy of the distributed ledger.

Blocks, responsible for the naming of the blockchain, are an integral part of any blockchain platform. In Hyperledger Fabric they are comprised of a header, a data section that contains one or more ordered transactions, and a trailer that contains metadata. The blocks are connected using cryptographic methods; more specifically, a block's header will contain a hash of the previous block.

Figure 5–3 illustrates a diagram of a block and a transaction respectively, indicating what are the contents of the block, and transaction(s) found within the block, in more detail to aid with the visualization of the transaction flow and the ordering of transactions into blocks.

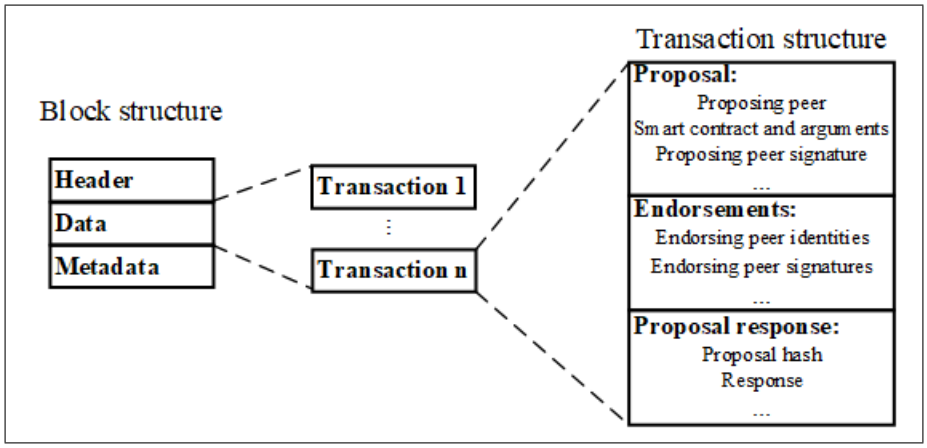



Figure 5–3: Block and transaction structures

Using Hyperledger tools, a business network is deployed on Fabric, which implements the architecture of the system. The business network contains assets, participants, and transactions, the combination of which is called the model of the network. It also contains transaction functions, also called smart contracts, and access control rules. An example of a network asset is a patient's medical record. An example of a network participant is a user of the system, such as a patient. Also, an example of a network transaction is updating the patient's medical record using the immutability property found in blockchains. The participants are essentially images of the users within the network, and users can be associated with an identity. The identity is used to connect to the business network and is subject to the specified access control rules mentioned above. An example of access control would be that a patient identity may only view information related to itself, whereas a medical center would have access to all its patients.

Access to the business network needs to be available to the participants and to do so, the network is exposed as a Representational State Transfer (REST) Application Program Interface (API), using a REST server. The REST server allows a web application to interface with the business network and Hyperledger Fabric. The web application is used by the users to access the blockchain-based data transmitting and storage system, where they sign in to the business network with their identity, through the REST server.

## 5.4 Implementation of the proposed blockchain-based eHealthcare system interoperating with WBANs

To evaluate the proposed blockchain-based eHealthcare system, a miniBEE platform which contains a Xilinx Vertex 6 XC6VSX475T FPGA and runs CentOS, one

smartphone with Android operating system, and two PCs have been utilized to simulate all the roles in the proposed system. The miniBEE platform is running the WBANs transceiver specified by the IEEE 802.15.6 standard to simulate a patient as the front-end in WBANs environment, while the blockchain network is deployed on the Hyperledger Fabric platform.

### 5.4.1 Implementation of the blockchain in the proposed system

For the blockchain-based data transmitting and storage module evaluation, the Hyperledger Fabric platform version 1.0 is used. Additionally, the Hyperledger Fabric Composer framework is used to model and deploy the business network on Fabric, and Hyperledger Composer REST server is used to expose the business network as a REST API. For the web application, Node-RED is used.

For the implementation, Fabric is configured as one peer node belonging to one organization, one Certificate Authority (CA), and one orderer node. The orderer is running the SOLO ordering service, which is a simple non-production ordering service consisting of a single process. Consequently, there is no real consensus taking place as there is a single orderer node, however it is the preferred approach for development and testing.

All the Fabric processes (peers, certificate authority, and orderer) ran inside Docker containers. The containers, the Fabric Composer framework, and REST server all ran in an Ubuntu 16.04 LTS 64-bit virtual machine.

In the model of the business network deployed on Hyperledger Fabric describing the architecture of the blockchain-based data transmitting and storage system, six participants, one asset, and four transactions are defined. The transaction functions

are implemented in javascript, which is also called chain code or smart contracts. Access control rules are also specified, allowing or denying access to resources depending on the identity of the user, which is tied to a specific participant.

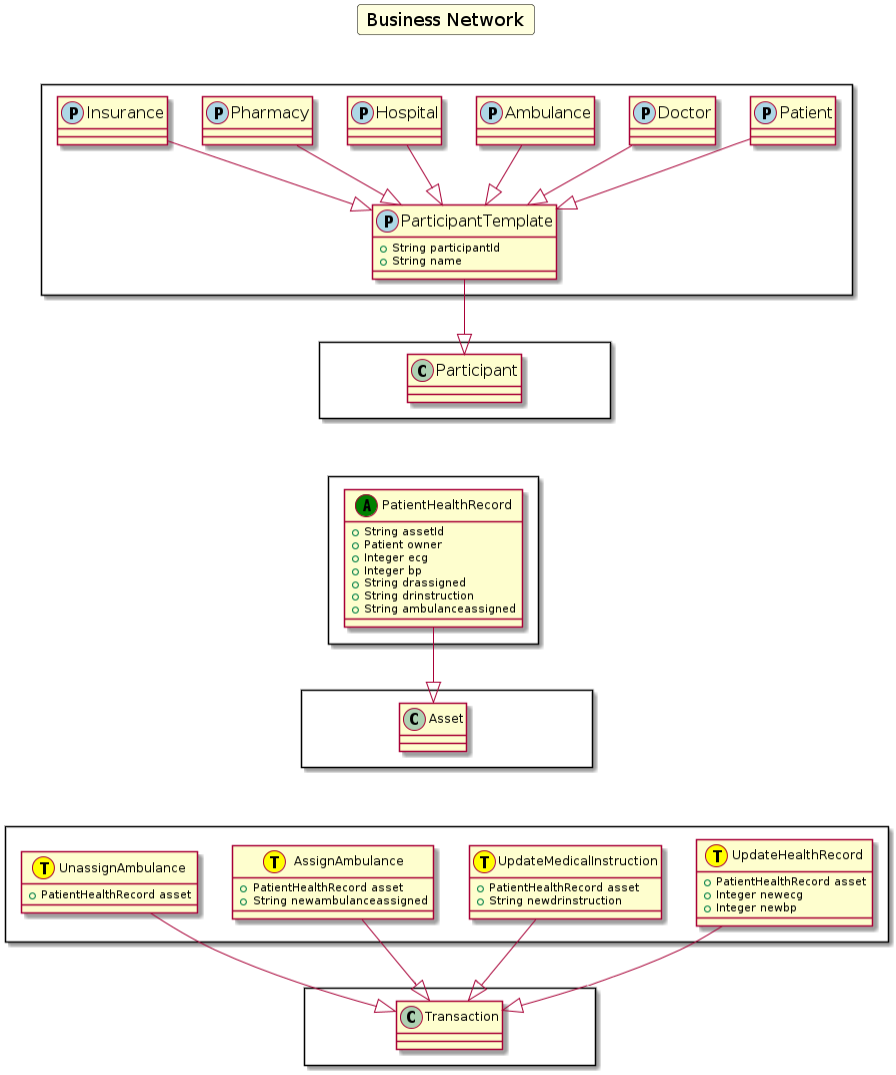



Figure 5–4: UML class diagram showing the business network model

The participants are doctors, patients, medical centers, hospitals, emergency services, ambulances, medicament suppliers, pharmacies, and insurance companies. The asset is the patient health records, which contain information on both the patients and their doctors. Patients can submit transactions to update health records with health information. Appropriate doctors can submit transactions to update the health records with medical instructions, as well as assign and remove an emergency service participant to a patient. The insurance companies are aware of all medical instruction submitted. Any payments that may be required are automatically made when a medical instruction is submitted, as part of the same transaction. Medicaments are also supplied if necessary. The insurance companies can automatically pay when needed, and they also have access to a plethora of information which can be used to form statistics. Meaningful statistics are extremely powerful for insurance companies, as they can be used to accurately compute risks and premiums by actuarial principles.

The business network is defined in the Hyperledger Composer Modeling Language, which is used to describe the participants, assets, and transactions. A Unified Modeling Language (UML) class diagram of the business network model was created, using PlantUML, which is featured in Figure 5–4. In the diagram, the network is modeled to clearly show participants, assets, and transactions. A participant (such as a patient) or asset (such as the patient's health record) that is added to the network will implement an instance of the respective participant or asset (Patient or PatientHealthRecord) found in the model.

Access control rules are used to allow or deny access as needed. For example, patients may only view their own health record, whereas doctors may only view their patients' health records. A medical center may view the health records of all the patients that use it. The emergency services temporarily gain or lose access to patient health records, as necessary. Medicament supplies may view health records of patients that require medicaments, however less personalized information such that they cannot, for instance, view the name of a patient. Insurance companies may access all the data of their customers once the patients are having medical services. The above properties can be found described in the Hyperledger Composer Access Control Language and control the network by providing declarative access control over the modeled elements. They can be used to determine which users can read, create, update, or delete elements in the business network. Participant instances are associated with identities, which essentially are the users that can perform operations on the network, and subject to the access control rules.

### 5.4.2 Implementation of the WBANs in the proposed system

The WBANs in the proposed system are implemented by the MiniBEE4 SDR platform for evaluation purposes. The Virtex-6 XC6VSX475T Xilinx FPGA embedded in the MiniBEE 4 platform runs a baseband transmitting module and a receiving module of WBANs, two Square-Root Raised Cosine (SRRC) filters, a digital down converter (DDC), and a low-pass filter. Meanwhile, the FMC111 RF front end is embedded in the platform, which consists of a Digital Analog Converter (DAC), an upconverter, an amplifier, a Low Noise Amplifier (LNA), a down converter, a band-pass filter, and a digital-analog converter, which are used to process the RF

transmission. Two omnidirectional antennas have been utilized as the transmitting antenna and receiving antenna. Furthermore, an MCU has been connected to the FPGA to generate and verify the source data. The architecture of the implementation of WBANs in the proposed system is demonstrated in Figure 5–5.

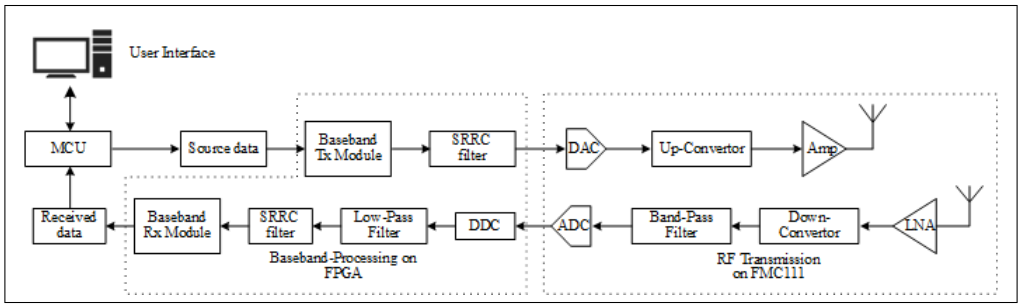



Figure 5–5: Implementation of WBANs in the proposed system

## 5.5 Evaluation of the proposed system

The evaluation environment of the proposed blockchain-based eHealthcare system interoperating with WBANs is performed as shown in Table 5–1. A web application has been provided to every role in the system to have access to the blockchain-based data transmitting and storage system. Detailed evaluation has been separated into two parts: the evaluation of the blockchain-based data transmitting and storage system, and the evaluation of WBANs.

### 5.5.1 Blockchain-based data transmitting and storage in the proposed system

The average latency to process a transaction was measured to be approximately 2350 milliseconds per transaction. This is the latency to submit a transaction, all the way from aggregating the data in a sensor node hub and sending it through the REST API to the blockchain back-end, to the proposal, endorsement, and ordering

Table 5–1: Evaluation environment

| Roles | Evaluation Environment |
|---|---|
| Patients and WBANs | BEECube MiniBEE4 |
| Blockchain-based Data Transmitting and Storage | Hyperledger Fabric |
| Doctors | PC |
| Medical Center(s) | PC |
| Emergency Service | PC |

of the transaction into a block. This latency would theoretically allow up to 51 users to submit transactions to the system once every two minutes each, assuming no transactions ever overlap. This is also only taking into consideration biomedical data that updates patient health records, other transactions would need to execute too.

This number is influenced by various parameters such as the number of peers, the number of machines the peers are running on, as well as the computational power of the physical, or virtual, machines themselves, or even network latency in the case of multiple physical machines. The most important parameters, however, are the ordering service used in Hyperledger Fabric, and its configuration. As discussed above, the SOLO ordering service is centralized and consists of a single process running on a single node. As such, there is correspondingly low availability and scalability, which hinders performance. SOLO is therefore acceptable for testing purposes, but not for a production environment.

Further, the achieved performance is insufficient to support a realistic situation of a regular sized medical center. Therefore, optimizations in the blockchain would be necessary. for instance, tweaking the blockchain ordering service to create blocks

more frequently could improve performance. Moreover, Hyperledger Fabric employs MultiVersion Concurrency Control (MVCC) to prevent the double spending problem. Therefore, overlapping transactions are not executed. Workarounds for this could be implementing a queue between the users and the blockchain back-end, which ensures that transactions will execute until they succeed. Another performance gain could be achieved by performing bulk reads/writes during MVCC validation and commit [88]. [88] showcases more complete work regarding Hyperledger performance and optimizations.

### 5.5.2 WBANs in the proposed system

As mentioned before, the implementation of the WBANs part of the proposed system is performed on the BEEcube miniBEE4 platform. The setup of parameters for the FMC111 RF front end is demonstrated in Table 5–2, where the 1800 MHz radio frequency and pi/4-DQPSK modulation are defined in IEEE 802.15.6 standard. The other parameters are set up according to the practical system requirements. The detailed evaluation results regarding the utilization of LUTs, registers, memory, and Digital Signal Processing Units (DSPs) are illustrated in Table 5–3. First, it can be found that the proposed design utilizes a quite low hardware resource, which means, on one hand, the SDR platform is quite extensive for further improvement. However, the proposed design could be implemented with low hardware cost in a future ASIC chip.

Meanwhile, the symbol rate of the WBANs implementation achieves 31.25 Msps, which means the data rate is up to 62.5 Mbps. As the centralized side has been set up to perform transactions every two minutes. The size of biomedical data in

Table 5–2: System parameters

| SDR Evaluation Platform | BEEcube miniBEE4 |
|---|---|
| Radio Frequency | 1800MHz |
| Midle Frequency | 30.72MHz |
| ADC Sample Rate | 250Msps |
| Modulation | $\pi/4$ DQPSK |
| Baseband Symbol Rate | 31.25Msps |

Table 5–3: Hardware resource utilization of the baseband test demo module

| Hardware Resources* | Specifications | Utilization Ratio |
|---|---|---|
| LUTs | 14,805/297,600 | 4% |
| Registers | 11,707/595,200 | 1% |
| Memory | 81/1,064 | 7% |
| DSPs | 190/2,016 | 9% |
| Clock Frequency | 250MHz | – |

$*$ FPGA platform: Virtex-6 XC6VSX475T Xilinx FPGA.

the eHealthcare system is between 10k bits to 1M bits, the data rate that can be supported in WBANs is more than sufficient to interoperate with the blockchain-based system, and can even be extended in future for larger transactions.

As can be seen from the evaluation results, the WBANs implementation of the proposed blockchain-based eHealthcare system has relatively low hardware resources utilization. Meanwhile, the symbol rate and frequency of the WBANs implementation demonstrates that it could interoperate with the blockchain-based data transmitting and storage system in the proposed system properly since the centralized side has been set up to perform transactions every two minutes.

## 5.6 Summary of the chapter

In this chapter, a blockchain-based eHealthcare system interoperating with WBANs, which follows the specifications in the IEEE 802.15.6 standard, has been proposed. The evaluation results demonstrate that the proposed system has the advantages of low hardware utilization, high-security protection level, and stable performance. Therefore, the proposed eHealthcare system has great potential to be applied in modern medical systems.

In future, more research will follow in this project. First, research regarding improving the blockchain network of the system will be undertaken, since the blockchain network can only support a maximum of 51 users for now, which is not suitable for a medical center with many patients and doctors. Meanwhile, more practical evaluations in the medical institutions will also be investigated to explore the performance of the proposed system in practical medical circumstances.

# CHAPTER 6
# A Software Defined Radio Evaluation Platform for WBAN Systems

In recent years, the WBANs concept has attracted significant academic and industrial attention. WBANs specifies a network dedicated to collecting personal biomedical data from advanced sensors that are then used for health and lifestyle purposes. In 2012, the 802.15.6 WBANs standard was released by the IEEE, which regulates and specifies the configurations of WBANs. Compared to the prevailing wireless communication protocols such as Bluetooth and Zigbee, WBANs standard has the advantages of ultra-low power consumption, high reliability, and high-security protection while transmitting sensitive personal data. Based on the specifications of the standard, several implementations have been published. However, in terms of evaluations, different designs were implemented in proprietary evaluation platforms, which may lead to unfair comparison. In this chapter, An SDR evaluation platform for WBAN systems is proposed for evaluating the RF channel specified in the IEEE 802.15.6 standard. An NB communication protocol demonstration with a security scheme in WBANs has been performed to successfully validate the design in the proposed evaluation platform.

## 6.1 Introduction of the chapter

Based on the data provided by CIHI, the average health expenditure for every individual in Canada is $6,604$ Canadian dollars in 2017, which requires 11.5% of the overall GDP, up from only 7% of the GDP in 1975. In other words, Canadians spent

4.5% more of their wealth for healthcare over the past 43 years [17]. Meanwhile, according to the report provided by Bacchus Barua from the Fraser Institute [10], the average waiting time for consulting medical professionals was 21.2 weeks in 2017 in Canada due to the shortage of medical professionals, even though they have spent a huge amount of their income on healthcare. Therefore, there is a strong demand for economical and efficient healthcare solution, which is also capable of addressing the shortage of medical professionals. One such solution can be a secured eHealthcare system which can not only monitor the physical conditions of the patients remotely but also analyze the potential physical issues the patients are facing, and provide feedback to them, as demonstrated in Figure 1–1.

By benefiting from the rapid development of modern technology, increasing types of biomedical data can be collected from patients and transmitted to the cloud for further data processing and storage. This is especially true with the rapid growth in advanced biomedical sensors, such as EEG and ECG sensors [84] and blood pressure sensors [112], as well as wireless networking, such as 5G and BLE. However, there are two potential issues that still restrict the development of eHealthcare systems [65], [60]. First, the sensors on humans are extremely power-sensitive, especially the implanted sensors with limited power supply and inconvenience of battery change. The most commonly utilized wireless communication technologies in the proposed sensors are Bluetooth and Zigbee, which are not dedicated and optimized for biomedical data transmission. Second, the data collected from patients is private and critical, which could cause serious problems if the information tampering. Hence,

Table 6–1: Power comparison among different wireless communication technologies [65]

| Wireless Communication Technologies | Power (mW) | Battery life |
|---|---|---|
| Bluetooth | 5 to 100 | 1 day to 4 weeks |
| Zigbee | 5 to 60 | 3 days to 5 weeks |
| WBANs | 0.1 to 5 | 6 weeks to 12 months |

an efficient and unique security scheme is also necessary for wireless communication in the eHealthcare system.

WBANs, illustrated in Figure 1–2, have attracted huge academic and industrial attention in recent years, because they define the shared communication infrastructure for wireless data transmission among sensors and other devices. In 2012, IEEE released the 802.15.6 WBANs standard, which specifies and regulates the detailed configurations of WBANs. Based on the specifications of the IEEE 802.15.6 WBANs standard, multiple hardware-based and software-based implementations of WBANs have been proposed [101], [102], [23]. The evaluation results of the implementations illustrate that WBANs have advantages in power consumption, privacy protection, and efficient communication for biomedical data. For instance, the power consumption of WBAN systems is between 0.1mW to 5mW approximately when the transmitting data rate is 1 Mbps, while for the same transmitting data rate, Bluetooth consumes between 5 mW to 100 mW approximately. In this case, the battery can last approximately 1 year in WBAN systems, while it can only last less than a month in Bluetooth systems [65] as illustrated in Table 6–1.

However, since the IEEE 802.15.6 standard supports three types of communication (NB, UWB, and HBC), and each communication is corresponding to various

transmission specifications such as encoding methods, modulations, and transmission frequencies, the designs were implemented in different platforms for evaluation purposes. However, evaluating different implementations of WBANs in various platforms could cause certain issues. On the one hand, the evaluation results are affected by different configurations of the platforms, such as the performance of the FPGA, Random-access memory (RAM), and Read-only memory (ROM), which leads to unfair comparisons among different designs. On the other hand, establishing evaluation platforms for every individual implementation of WBANs is not only time consuming for the researchers and engineers, but also increases the complexity of the design. Since each RF front end, design and fabrication will take many months, a platform is needed that can drastically speed up the evaluations.

The motivation of this research is to provide a rapidly configurable SDR evaluation platform for WBAN systems, which not only can provide test cases that can help evaluate different modules in different circumstances (e.g., the BER for different distances), but also be reproducible in multiple implementation platforms. To provide a wider benefit to the research community, all the source code for this SDR platform is posted to a publicly accessible GitHub repository. The SDR evaluation platform may be used to evaluate and prototype different applications, including but not limited to healthcare networks and vehicular networks [100], which were found to be good candidates for WBANs implementations.

Further, to ensure that the proposed SDR evaluation platform can be supported on various FPGA platforms (other than the MiniBEE), the verification has been

performed in Xilinx Kintex-7 FPGA KC705 Evaluation Kit, and Altera Arria 10 SoC Development Kit.

Our contributions are as follows. First, the procedure of designing and validating the WBAN systems is dramatically shortened by utilizing the proposed evaluation platform, since there is no need to build circuits for each specific WBAN system, especially when the transceivers take an exorbitantly long time to be developed in ASICs.

Second, it is more feasible for researchers to evaluate the real performance of a certain optimized module in the WBANs by simply replacing the module in the evaluation platform and comparing the performance. By selecting the appropriate hardware on which the evaluation platform can be implemented, which would be dependent on the application, and evaluating two different modules on it, module optimization can be carried out to a certain extent. At the same time, the evaluation platform can be implemented in different hardware, should a different application require that. Third, it provides a fair comparison platform to evaluate different designs for WBAN systems in RTL level, which eliminates the effects for different circuit synthesis technologies.

The rest of this chapter is organized as follows. Section 2 provides the background and previous work focusing on the IEEE 802.15.6 standard and the general specifications of the SDR testbed. Functionality, structure, and hardware components of the proposed evaluation platform for WBAN systems are detailed in Section 3. The implementation of the proposed testbed for WBANs and a demo performance

of a baseband processing module with a WBANs security scheme is shown in Section 4. Section 5 concludes the chapter and provides a future work guide.

## 6.2 Background and related work

The IEEE 802.15.6 standard specifies three types of communication: NB, UWB, and HBC. Each communication type defines various configurations for the network. However, the processing flow is similar for different communication in WBANs. As specified in the IEEE 802.15.6 WBANs standard [42], the transmission flow of WBANs is mainly separated into four parts, which are MAC layer, security scheme, PHY, and RF front end as shown in Figure 2–2. Initially, the MAC layer specifies the MAC frame format and the communication modes in the network [89], which requires an MCU to process. Afterwards, the security scheme needs to determine whether the link needs to be authenticated and encrypted, based on the security level of communication. The PHY involves the baseband processing module, where it processes the original binary data from the security scheme into a format that is suitable for processing in the RF front end, where it is physically transmitted. Precisely, the responsibility of the baseband processing module is the activation and deactivation of the radio transceiver, clear communication assessment, and data reception and transmission [89]. Last but not least, the RF front end converts the digital data into an analog signal modulated at the right frequency, passes the modulated signal to an amplifier, and transmits it by the antenna (vice versa for the receiver).

### 6.2.1 Specifications of IEEE 802.15.6

#### MAC layer of WBANs

Sitting above the PHY, the MAC layer of IEEE 802.15.6 is designed to control communication access. To do this, the MAC layer divides the entire communication into a chain of superframes through the hub (coordinator). At the boundary of these superframes, the hub chooses beacon periods of equal length to bound each superframe. If needed, one could shift the offset of the beacon period through the hub. The superframes will be normally sent in each beacon period [65], unless there is a restriction by regulations in the MICS band or the superframes are inactive. Figure 2–3 provides an overview of the structure of superframes in the standard. The superframe can be divided into three different components, the MAC header, the MAC Frame Body, and the FCS. With a length of 7 Bytes, the MAC header can be further divided into Recipient ID, Sender ID, WBANs ID, and Frame Control, which contains information such as protocol version, ack policy and so on. The MAC Frame Body has a variable length; it contains Low-Order Security Sequence Number, Frame Payload with selected types, and MIC. The last 2 bytes of a MAC frame is the FCS to detect possible errors in transmission. The standard specifies the CRC-16-CCITT sequence to be used in error detection. The CRC polynomial is shown in Equation 6.1, where $a_{15}$ is the LSB of the field, $a_0$ is the MSB, and $a_{15}$,$a_{14}$,...,$a_0$ are the binary coefficients.

$$G(x) = x^{16} + x^{12} + x^5 + 1 \tag{6.1}$$

**Security scheme of WBANs**

The IEEE 802.15.6 standard specifies three security levels for all communication in WBANs, Level 0, Level 1, and Level 2 respectively. Level 0 is unsecured communication, where neither authentication nor encryption is required. Public information, such as time stamps, which is neither critical nor private, could be transmitted at this security level. Meanwhile, the communication of security Level 1 contains private, but not critical data, such as names, ages, and locations. This data is not significant for the physical conditions of the patients; however, users would still not want to release it to the public. In these cases, authentication is required while encryption is not involved. In the cases of the most critical data, such as blood pressure, heart rate, and parameters for a pacemaker, it is a requirement for them to be transmitted at security Level 2. Both authentication and encryption are mandatory for Level 2 communication.

In terms of the methods implementing authentication and encryption, the standard specifies the certificate validation as the authentication method and ECC as the encryption method. Based on the specifications, multiple security schemes have been proposed to achieve the functionality of security protection of WBAN systems. Precisely, lightweight data authentication schemes have been proposed in [27] and [80], which achieved much lower power consumption than conventional WBANs security schemes. Moreover, [116] and [72] proposed data authentication and encryption methods by utilizing the data collected from the sensors to generate dynamic keys, which simplifies the system complexity of the security scheme while increasing the security level. Furthermore, an ASIC implementation of the security scheme for

WBANs has been proposed [102]. In this design, besides validating the certificate, there is a second phase for the authentication procedure called challenge-response phase to increase the security protection of the communication in WBANs.

**PHY of WBANs**

As mentioned before, in the specifications of the IEEE 802.15.6 WBANs standard, there are three types of communication that could be utilized in the communication of WBANs: NB, UWB, and HBC, respectively. As a typical case, the physical layer processing of NB communication is analyzed as follows.

The standard PPDU for NB is illustrated in Figure 3–1. Every PPDU contains three main components: the PLCP preamble, the PLCP header, and the PSDU.

• PLCP Preamble

As seen in Figure 3–1, the 90-bit PLCP preamble is the initial data package that needs to be sent for every PPDU to assist the receiver in data packet detection, timing synchronization, and carrier recovery. The data packet detection, timing synchronization, and carrier recovery are presented next.

• PLCP Header

Following the PLCP preamble, a 31-bit PLCP header that contains a 15-bit PHY header, a 4-bit HCS, and 12-bit BCH parity bits, can be found. The BCH code with 19 information bits and 12 parity check bits (31,19,2) is a shorter version of standard BCH code (63,51,2), which provides up to $t$=2 error bit correction capability. The purpose of the PLCP header is to provide the system configuration parameters related to the receiver.

The PHY header is constructed by a 3-bit RATE, 8-bit LENGTH, 1-bit BURST MODE, and 1-bit SCRAMBLER SEED, while two bits are reserved. The detailed encoding methods and the corresponding meaning of them are specified in the IEEE 802.15.6 standard.

- PSDU

The PSDU is the component that contains the data from the MAC layer. More precisely, it consists of a 7-byte MAC header at the beginning of the sequence, a 2-byte FCS at the end of the sequence, and a 0-255 byte MAC frame body in the middle containing the data. In this work, the MAC frame body length is fixed to 255 bytes to simplify the control logic of the transmitter.

The block diagram of the baseband transmitter is illustrated in Figure 6–1. According to the IEEE 802.15.6 standard, the modulation for the preamble, PLCP header, and PSDU is $\frac{\pi}{2}$-DBPSK, $\frac{\pi}{2}$-DBPSK and $\frac{\pi}{4}$-DQPSK, respectively.

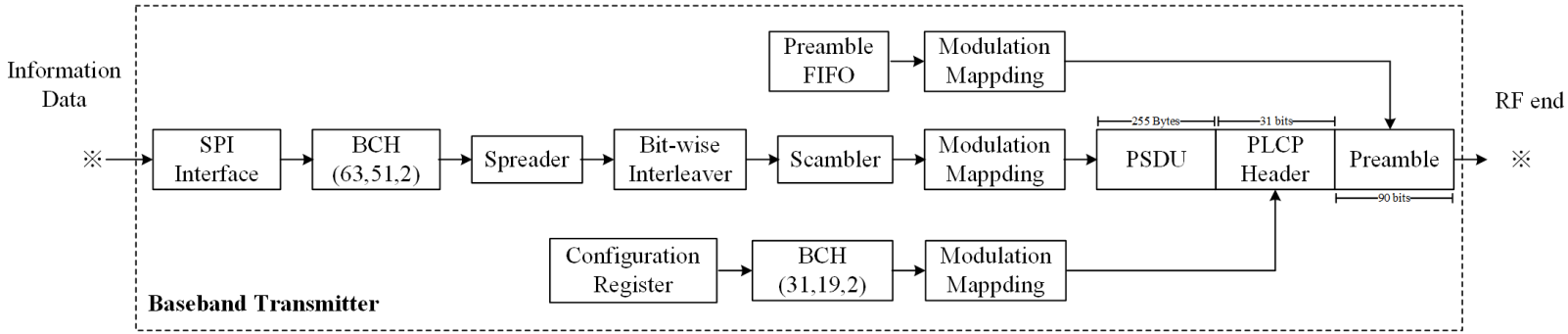



Figure 6–1: The block diagram of the baseband transmitter

### 6.2.2 Radio frequency characteristic of WBANs

The IEEE 802.15.6 standard covers a series of operating frequency bands: 402 MHz to 405 MHz, 420 MHz to 450 MHz, 863 MHz to 870 MHz, 902 MHz to 928 MHz, 950 MHz to 958 MHz, 2360 MHz to 2400 MHz, and 2400 MHz to 2483.5 MHz. Each frequency band includes several sub-channels which are shown in Table 2–2, where $g_1(n_c)$ and $g_2(n_c)$ are mapping functions used in the 420 MHz to 450 MHz and 863 MHz to 870 MHz frequency bands, respectively.

$$g_1(n_c) = \begin{cases} n_c, & 0 \leq n_c \leq 1; \\ n_c + 6.875, & 2 \leq n_c \leq 1; \\ n_c + 13.40, & n_c = 5; \\ n_c + 35.025, & 6 \leq n_c \leq 7; \\ n_c + 40.925, & 8 \leq n_c \leq 9; \\ n_c + 47.250, & 10 \leq n_c \leq 11; \end{cases} \tag{6.2}$$

$$g_2(n_c) = \begin{cases} n_c, & 0 \leq n_c \leq 7; \\ n_c + 0.5, & n_c = 8; \\ n_c + 1, & 9 \leq n_c \leq 12; \\ n_c + 1.5, & n_c = 13; \end{cases} \tag{6.3}$$

Based on the different bandwidth on these frequency bands and using the corresponding baseband parameter configuration, the data transmission rate is shown in Table 6–2.

Table 6–2: Data rate supported on each frequency band

| 402 to 405 MHz | 420 to 450 MHz | 863 to 870 MHz<br>902 to 928 MHz<br>950 to 958 Mhz | 2360 to 2400 MHz<br>2400 to 2483.5 MHz |
|---|---|---|---|
| Data rate (kbps) | | | |
| 75.9 | 75.9 | 101.2 | 121.4 |
| 151.8 | 151.8 | 202.4 | 242.9 |
| 303.6 | 187.5 | 404.8 | 485.7 |
| 455.4 | | 607.1 | 971.4 |

### 6.2.3 SDR testbed

The traditional industrial process of developing a digital communication system is to use an ASIC to perform the RF test. However, despite having the advantages of great performance, low power, and reduced footprint, using an ASIC, on the other hand, raises a high non-recurring cost and dramatically increases the development time. Unlike the ASIC implementation, SDR testbeds provide users with great flexibility to evaluate the RF performance of a certain design. For a common SDR system, the data processing task is performed by a digital signal processor (DSP) or by an FPGA. Due to the programmable nature of the DSP and FPGA, users working with SDR platforms have the ability to change the parameters of the system based on their requirements [74].In industry, SDR testbeds have been widely adopted as verification tools in wireless communication by the researchers working with other technologies such as Long Term Evolution (LTE) [78], WLAN [5], Bluetooth [76], and 5G technologies [108]. For instance, in the article [57], the authors proposed a new design architecture to provide effective spectrum management for 5G wireless

networks by applying it on an SDR platform. On the contrary, there is still no existing SDR evaluation platform for the latest IEEE 802.15.6 standard. Meanwhile, the IEEE 802.15.6 standard defined a wide range of frequency channels and multiple modulation methods for applications under different circumstances [89]. This highly adaptive nature raises the need for an equally flexible evaluation platform. Due to the configurable nature of the SDR platform, switching among different frequency channels and modulation methods can be achieved easily, which was earlier impossible without manufacturing multiple ICs that implement different configurations.

## 6.3 Proposed SDR evaluation platform for WBAN systems

### 6.3.1 Functionality description

As mentioned in Section 2, WBANs supports three types of communication, namely NB, UWB, and HBC channel. Various methods of encoding, operation frequency, modulation, and other communication parameters shall be utilized in different communication in WBAN systems. Further, the security scheme could also vary based on the security level of the communication. Therefore, for the evaluation purpose of WBAN systems, all supported configurations including methods of encoding and decoding, operation frequency, methods of modulation, and specific security scheme, need to be implemented in the evaluation platform. In this section, an SDR evaluation platform for WBAN systems is proposed that supports all the communication specified in the IEEE 802.15.6 standard utilizing RF as a carrier. In addition, since HBC does not utilize RF as the communication carrier, it is not supported in

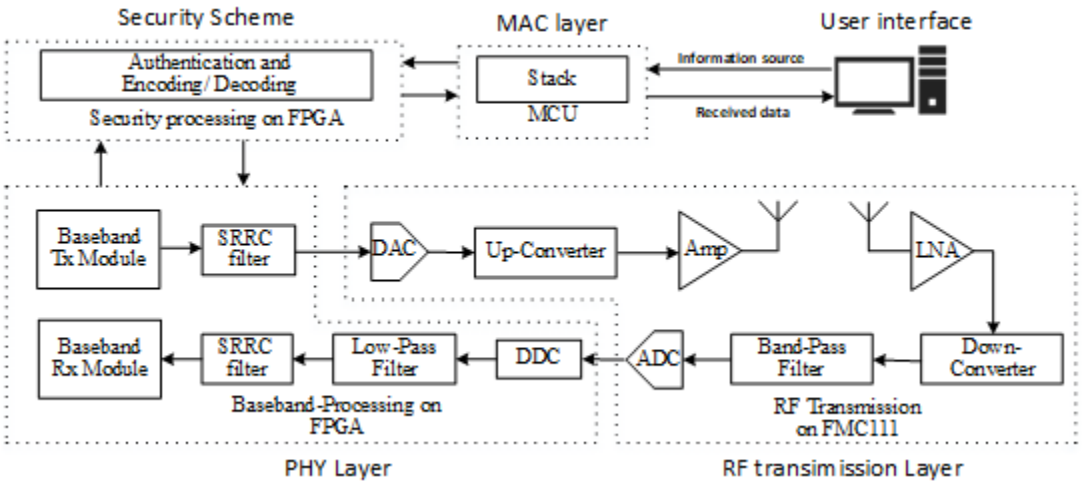



Figure 6–2: Architecture overview of the proposed SDR platform

the proposed evaluation platform. The detailed architecture and specifications are given in the subsections to follow.

### 6.3.2 Hardware architecture

In the proposed SDR evaluation platform, the information source generated from the user interface can be transmitted through three different hardware components in a designated sequence. As illustrated in Figure 6–2, after the information is sent from the user interface, it will be first transmitted into the protocol stack for frame formation implemented in the MCU. Then, these frames will be authenticated and encoded following the given security scheme of the IEEE 802.15.6 standard on an FPGA. Once the encoding process is done, the encrypted data goes into the baseband processing step implemented in an FPGA. Here, the encrypted message will be modulated and filtered through an SRRC filter under the specified settings. After that, this signal will be passed into an FMC 111 RF board. In this RF module,

the digital signal will first be converted into an analog signal and will then be stepped up to the radio frequency for transmission through the antenna. On the receiver side, once the antenna receives the transmitted signal, it will downconvert the RF signal to a medium frequency (MF) of 30.72 Mhz to meet the relatively low sampling rate of the analog to digital converter (ADC). After getting the digital signal, the signal will be passed into the DDC to shift the MF down to the baseband. Once the baseband signal is obtained, it is passed through a low-pass filter to filter out the harmonic frequencies. The remaining processes are just the inversion of the previous processes. Once the signal is passed through the SRRC filter, which is compatible with the sending end SRRC, it is demodulated in the baseband receiver module. Then, the security scheme applied to FPGA decodes the data and sends it to the protocol stack for de-framing. Finally, the extracted data is sent back to the user interface.

The detailed configurations of the proposed evaluation platform are demonstrated in Figure 6–3. As can be seen from the figure, every individual block is reconfigurable as needed. Once the configuration of a certain block is determined, the corresponding modules will be activated, while other modules which are not utilized will be disabled to reduce the hardware cost of the platform.

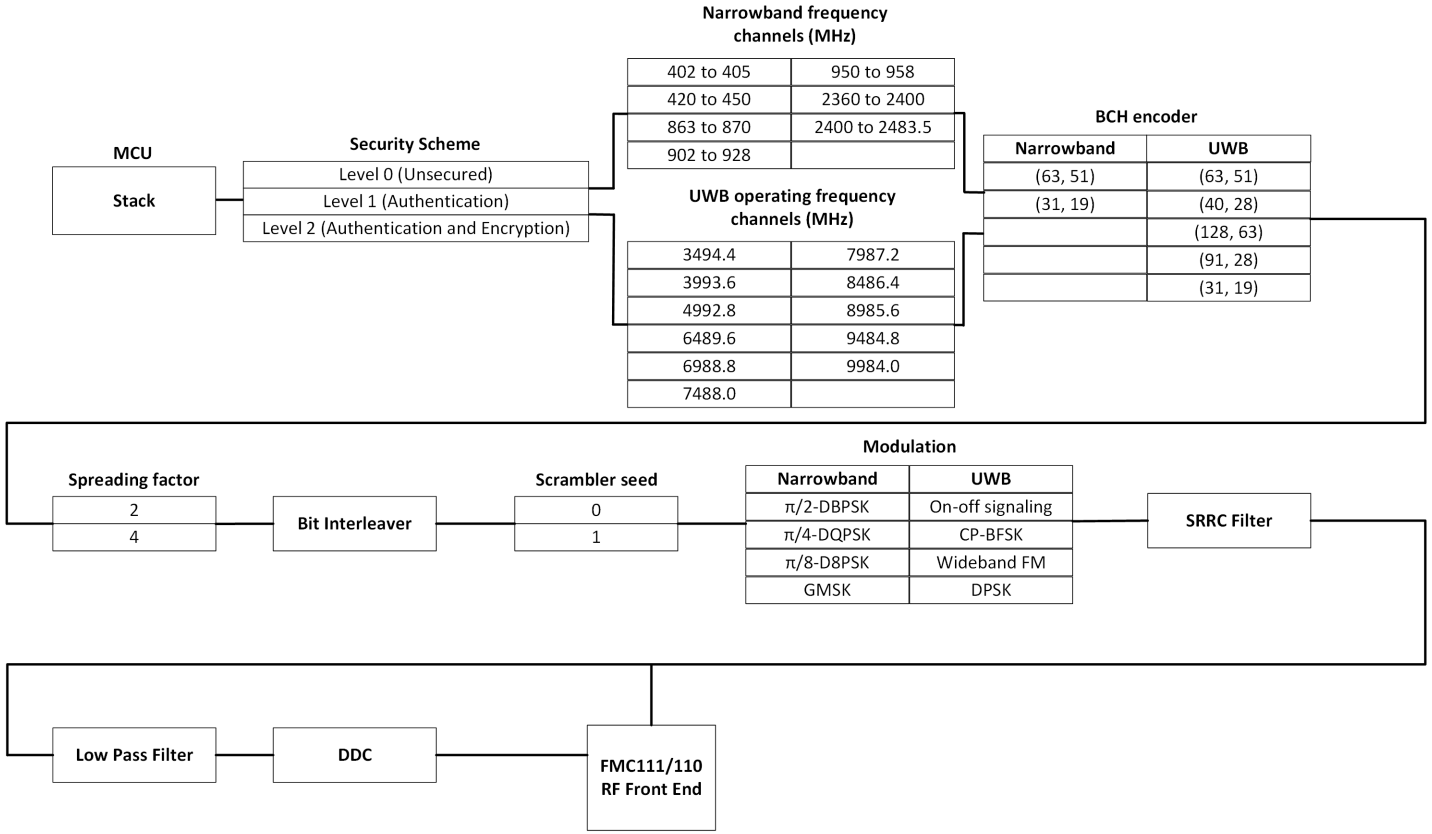



Figure 6–3: Implementation architecture of the proposed SDR platform

For example, assume that the security level of a certain communication has been determined to be Level 1, which requires authentication but not encryption. In this case, the authentication module of the security scheme in the evaluation platform is activated, while the encryption module is disabled. Based on the types of communication, the different operating frequency is distributed. For NB communication, the proposed evaluation platform supports 7 RF bands from 400 MHz to 2.4 GHz, while it also supports 11 RF bands from 3494.4 MHz to 9984.0 MHz for the UWB communication. Meanwhile, even though both NB and UWB utilize BCH as the coding method for communication, there are still various configurations for them. The proposed platform supports all the configurations for BCH encoding and decoding required by the standard as demonstrated in the figure. Moreover, there are 8 methods of modulation that can be configured in the platform; $\frac{\pi}{2}$-DBPSK, $\frac{\pi}{2}$-DBPSK, $\frac{\pi}{4}$-DQPSK, and GMSK for NB communication and On-off signaling, CP-BFSK, Wideband FM, and DPSK for UWB communication. The proposed evaluation platform is sharing the blocks for spreading factor, bit interleaver, scrambler seed, SRRC filter, low pass filter, and DDC for both NB and UWB communication, since they have identical configurations.

## 6.4 Implementation and demonstration

### 6.4.1 Implementation architecture of proposed evaluation platform for WBAN systems

The proposed SDR evaluation platform is implemented on a MiniBEE4 platform provided by Canadian Microelectronics Cooperation (CMC). The MiniBEE4 contains a Xilinx Virtex-6-XC6VSX475T FPGA connected with a configurable FMC111/110 RF front end, and a personal computer with CentOS running in it. In addition, two

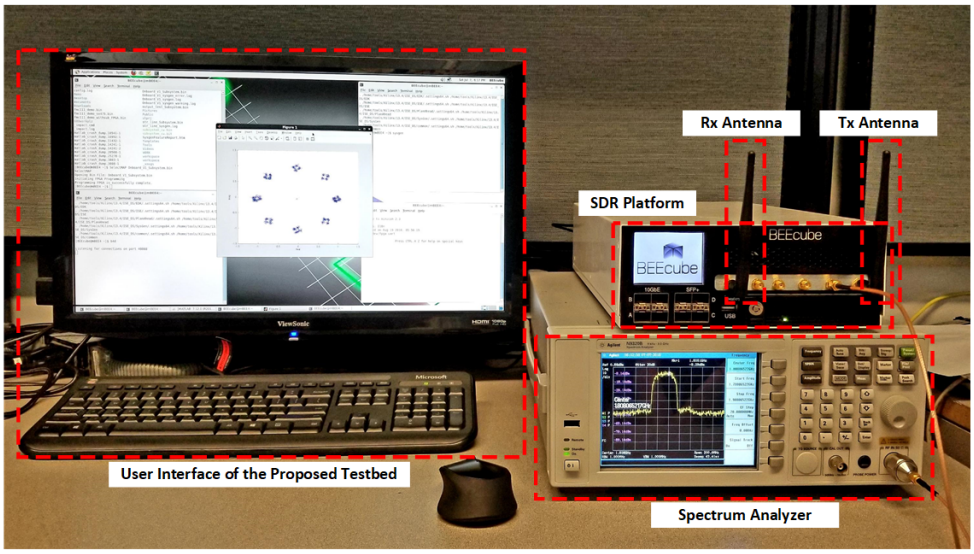



Figure 6–4: Demonstration of the proposed SDR evaluation platform for WBAN systems

isotropic antennas are attached to the RF front end. At the same time, an Agilent Infiniium DSA80000B spectrum analyzer is utilized to determine the frequency characteristics and verify the performance of the RF front end, as shown in Figure 6–4.

The User Interface (UI), connected with the MiniBEE4 SDR Platform, identifies the information source and received data, while the stack (MAC layer) is running in the CPU of the PC. The security scheme that contains an authentication module and encryption module is implemented in the FPGA, while the reconfigurable baseband processing module of the PHY (PHY) is also performed in the integrated Xilinx Virtex-6-XC6VSX475T FPGA.

In terms of the configurations of the RF front end found in the physical layer, a typical configuration of the RF channel is defined as shown in Table 6–3. Since the

Table 6–3: RF front end configuration

| FMC111/110 | Value |
|---|---|
| Radio Frequency | 1800MHz |
| Midle Frequency | 30.72MHz |
| ADC Sample Rate | 250Msps |
| Baseband Symbol Rate | 31.25Msps |

MiniBEE4 platform integrates a reconfigurable FMC111/110 RF front end, all the required operation frequencies specified in the IEEE 802.15.6 standard are supported and can be reconfigured through the RF setup.

### 6.4.2 Demonstration of evaluating a baseband processing module with a security scheme for WBANs performed in the proposed design

To further evaluate and verify the functionality of the proposed SDR evaluation platform for WBAN systems, a baseband processing module [101] with a security scheme [102] designed for WBANs has been implemented and evaluated in the proposed evaluation platform. Validating the RF channel functionality in various scenarios was the primary interest.

In terms of the demonstration, to assess the modulation scheme, Figure 6–5 demonstrates the constellation map for four cases. To be more precise, initially, there is a short distance between the two antennas (1 meter), and the constellation map from the receiver is shown as Figure 6–5 (a). It can be observed that the transmission quality could be guaranteed at 1-meter distance. Afterwards, a longer distance between two antennas (2 meters) is applied, and Figure 6–5 (b) illustrates the constellation map for that scenario. In this case, even though the transmission quality seems not as good as that in Figure 6–5 (a), the bit error rate can be further

improved by the BCH decoding methods. Moreover, in the circumstance of Figure 6–5 (c), a practical transmission link, where the maximum frequency offset between the transmitter and the receiver is specified in the standard (20 ppm), is considered. Last but not least, after the frequency offset correction, the constellation map is demonstrated in Figure 6–5 (d) which shows satisfying transmission performance. The overall transmission performance is expressed by the BER vs SNR for different modulation methods, as shown in the left side of Figure 6–6. The pink line, which is mostly overlapped with the blue line, is the performance result running in the proposed evaluation platform, which matches the simulation results.

To improve the performance of the communication in WBAN systems, multiple BCH decoding methods are applied to replace the original hard-decision decoder specified in the IEEE 802.15.6 standard. Therefore, hard-decision decoding, soft-decision decoding, and maximum-likelihood decoding methods for BCH (63,51) configurations have been simulated as demonstrated on the right side of Figure 6–6. The blue line is the performance results, BLER vs $E_b/N_0$, running in the proposed evaluation platform for the soft-decoding method, which meets the simulation results.

Furthermore, Table 6–4 demonstrates the hardware cost of implementing the baseband processing module in the proposed evaluation platform for WBAN systems. Moreover, the security scheme proposed in [102] has been utilized and implemented in the evaluation platform as the authentication and encryption module for the demo communication. The communication level is set to Level 2, which requires both authentication and encryption. Hardware utilization of the security scheme performing in the proposed evaluation platform is shown in Table 6–5. It could be found that

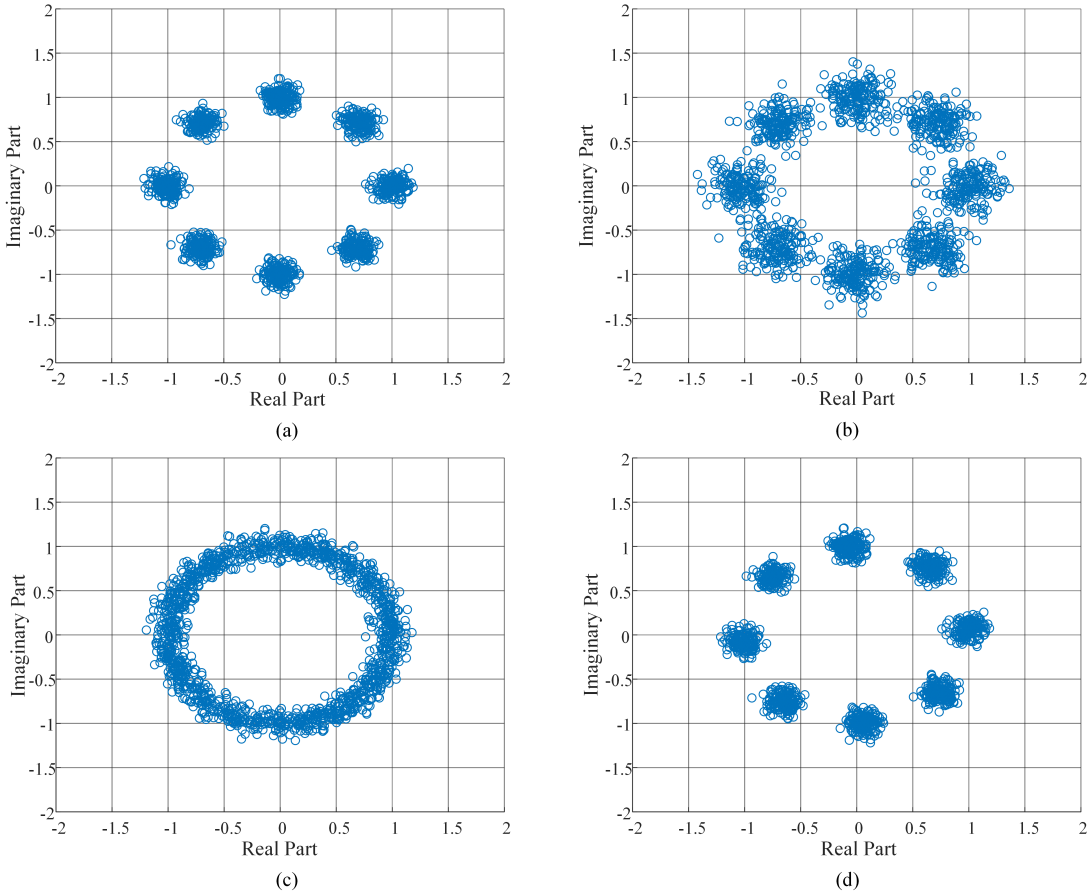



Figure 6–5: Constellation maps performed in the proposed evaluation platform for [101] ((a) Short distance; (b) Long distance; (c) Frequency-offset (max. 20 ppm. in IEEE 802.15.6); (d) Corrected frequency-offset)

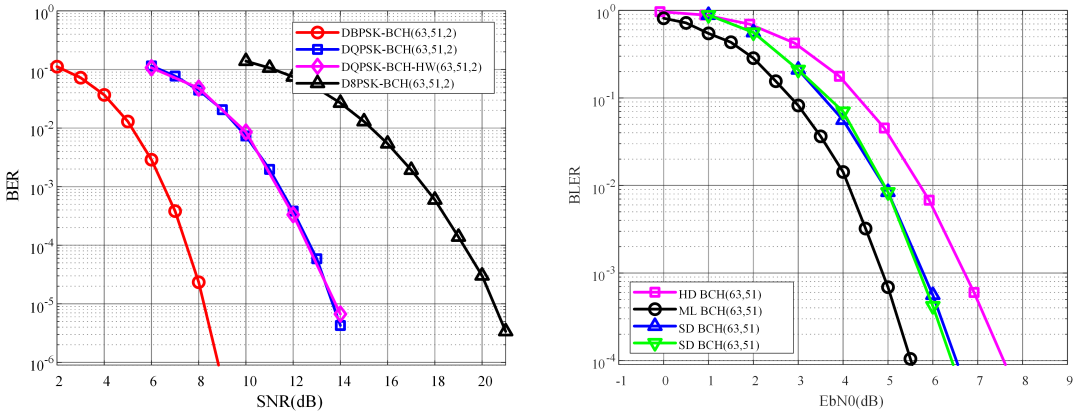



Figure 6–6: Communication performance executing in the proposed SDR evaluation platform for WBAN systems

Table 6–4: Hardware utilization of the baseband processing module performed in the proposed evaluation platform for WBAN systems

| Hardware Resources | Resources Utilized | Utilization Ratio |
|---|---|---|
| LUTs | 14,805/297,600 | 4% |
| Registers | 11,707/595,200 | 1% |
| Memory | 81/1,064 | 7% |

the FPGA platform hardware resource utilization is quite low, which means that the SDR platform is able to support more complicated functional tests and validations at the same time.

### 6.4.3 Discussion

For NB communication, the proposed evaluation platform supports 7 RF bands from 400 MHz to 2.4 GHz. However, for the UWB communication, 11 RF bands from 3494.4 MHz to 9984.0 MHz with 499.2 MHz bandwidth, as shown in Table 6–6, cannot be covered by the FMC111 RF module. Meanwhile, both NB and

Table 6–5: Hardware utilization of the security scheme performed in the proposed evaluation platform for WBAN systems

| Hardware Resources | Resources Utilized | Utilization Ratio |
|---|---|---|
| LUTs | 13,186/297,600 | 4% |
| Registers | 113,94/595,200 | 1% |
| Memory | 121/1,064 | 11% |
| DSPs | 190/2,016 | 9% |

UWB utilize BCH as the coding method for communication. The proposed platform supports all the configurations for BCH encoding and decoding required by the standard. Moreover, there are 8 methods of modulation that can be configured in the platform; $\frac{\pi}{2}$-DBPSK, $\frac{\pi}{2}$-DBPSK, $\frac{\pi}{4}$-DQPSK, and GMSK for NB communication and On-off signaling, CP-BFSK, Wideband FM, and DPSK for UWB communication. The proposed evaluation platform is sharing the blocks for spreading factor, bit interleaver, scrambler seed, SRRC filter, low pass filter, and DDC for both NB and UWB channels, since they have identical configurations.

Table 6–6: UWB operating frequency bands

| Band Group | Channel number | Central frequency (MHz) | Bandwidth (MHz) | Channel attribute |
|---|---|---|---|---|
| Low band | 0 | 3494.4 | 499.2 | Optional |
| | 1 | 3993.6 | 499.2 | Mandatory |
| | 2 | 4492.8 | 499.2 | Optional |
| High band | 3 | 6489.6 | 499.2 | Optional |
| | 4 | 6988.8 | 499.2 | Optional |
| | 5 | 7488.0 | 499.2 | Optional |
| | 6 | 7987.2 | 499.2 | Mandatory |
| | 7 | 8486.4 | 499.2 | Optional |
| | 8 | 8985.6 | 499.2 | Optional |
| | 9 | 9484.8 | 499.2 | Optional |
| | 10 | 9984.0 | 499.2 | Optional |

## 6.5 Summary of the chapter

With the development of modern technology, it becomes possible to establish an eHealthcare system that increases the efficiency of conventional medical systems. As the most fundamental element in the eHealthcare system, WBANs provides an ultra-low power, reliable, and efficient wireless communication channel for the data exchanging between the sensors and a hub. At the same time, WBANs implementations can be found in other areas as well, such as that of vehicular networks [100].

However, the lack of an evaluation platform for WBAN systems increases the complexity of designing novel systems for WBANs. Furthermore, evaluating WBANs designs on various platforms could cause unfair performance comparison among different designs intended for the same application. In this work, an SDR evaluation platform implemented in MiniBEE4 is proposed that supports all the communication configurations specified in the IEEE 802.15.6 standard. Up to the best of our knowledge, this is the first such reported case of all functioning IEEE 802.15.6 RF channels. Moreover, a demonstration of NB baseband processing module with the security scheme is set up to verify the performed evaluation platform. The demonstration results proved that the proposed SDR evaluation platform is functional, reliable, and provides the capability to build larger WBANs configurations with more complexity.

In future, more research attention will be invested in a few additional topics. First, more RF channel cases, such as UWB communication channel evaluation will be performed exhaustively in the proposed evaluation platform for WBAN systems. Moreover, a more rigorous verification procedure to evaluate WBAN systems in

the proposed evaluation platform will be investigated, so that different designs for the same functionality in WBANs, such as conventional BCH decoder and high-performance BCH decoder, could have fair comparisons.

# CHAPTER 7
# Conclusions and Future Work

## 7.1 Conclusions

With the rapid growth of the aging population in the world, the inefficient conventional medical system is no longer sufficient for strong demands for having regular medical services. The concept of the eHealthcare system provides a feasible solution to address the huge medical demands. Compared to the traditional medical system, the eHealthcare system can support all stages of care for the patients including prevention, diagnosis, treatment, and follow up remotely all day long. However, establishing of the completed and mature eHealthcare system requires the research and investigation in the wireless communication protocols for medical data transmitting between the centralized devices and the sensors.

As the most fundamental element of an eHealthcare system, WBAN is dedicated to the wireless communication for biomedical data exchanging in short distance. It allows not only the patients but also the medical doctors to be aware of the physical status of the patients remotely all day long. Furthermore, based on the requirements and characteristics of the circumstances, IEEE 802.15.6 was released to regulate the communication in WBANs.

However, even though many advanced sensors have been proposed which can collect the biomedical data relatively accurate according to the standard, few attentions have been given to the topics of security, baseband processing schemes for

WBANs. In this dissertation, low power security techniques and baseband processing techniques for WBANs and corresponding ASIC implementations have been discussed. Meanwhile, a blockchain-based eHealthcare system interoperating with WBAN systems has been proposed to provide a higher-level data transmitting and storage system which could cooperate with WBANs. Compared to a traditional medical data system, it has the trusted data exchange and storage environment benefiting from the advantages of distributed storage and mechanism of achieving the consensus of the blockchain. Finally, to evaluate different WBAN systems in an identical testing environment, a unified SDR based evaluation platform for WBAN systems has been proposed.

In conclusion, the dissertation achieved the objectives laid out in Chapter 1. The performed work made a further step for the wider acceptance of WBANs. Concretely, the dissertation proposed and implemented a low power baseband processing ASIC for the PHY of WBANs. Also, a stochastic computing based BCH decoder has been proposed for optimizing baseband processing procedure. Afterwards, a hardware-efficient security scheme for WBANs, which is proved to against common attacks, has been proposed and implemented as ASIC to address the security concerns over highly private data that WBANs transfer. In addition, the dissertation proposed a dynamic encryption method by using the body channel characteristic values, which fits nicely within WBANs normal use cases and has extra safeguards. Moreover, the blockchain-based eHealthcare system interoperating with WBAN systems provides a potential solution for the issues of interoperability and automation of WBAN systems and existing medical services such as the medical professionals, pharmacies, insurance

companies, and emergency services. Finally, to provide a unified testing environment for various designs in WBANs, an evaluation platform for WBAN systems has been proposed in the dissertation.

## 7.2 Future work

Even though different parts and techniques in the WBANs have been discussed and proposed in the dissertation and the future work of each individual chapter has also been discussed, there are still few general missions as listed below could be accomplished in future for achieving the better performance of the communication protocol in WBANs.

The first is that the performance analysis for the ASICs of the security scheme and baseband processing needs to be investigated after the final fabrication. Since the fabrication process is usually a long-term procedure, which could take for more than 6 months, the proposed ASIC designs are still undergoing. Even though all the proposed design has been verified in the FPGA platform and synthesized in the fabrication CMOS technology, there still could be a potential minor performance difference between the synthesized results and the practical results.

Meanwhile, still caused by the fabrication issue, the analysis of side channel attacks shall be done in the future to verify the security performance of the security scheme for WBANs. Even though the side channel attack analysis has been accomplished in the FPGA platform which illustrates sufficient performance as expected, while it is still necessary to have the practical test.

Third, the potential issues caused by the cooperation among different modules in the WBANs transmission flow shall be investigated, such as the cooperation between

the MAC layer and security scheme, and the cooperation between the security scheme and PHY in WBANs.

Finally, this dissertation proposed a blockchain-based eHealthcare system interoperating with WBAN systems, which provides a more efficient and reliable eHealthcare system compared to conventional healthcare systems. However, even though it illustrates a lot of advantages, moving to this blockchain-based eHealthcare system could be challenging from the conventional healthcare systems. Therefore, more research shall be given to the simple transfer or compile from the traditional healthcare system to the blockchain-based eHealthcare system interoperating with WBAN systems.

## Author's List of Publications

***A. Journals:***

1. **Wang, Junchao**, Kaining Han, Zhiyu Chen, Anastasios Alexandridis, Zeljko Zilic, Yu Pang, and Jinzhao Lin. "A Software Defined Radio Evaluation Platform for WBAN systems." Sensors 18, no. 12 (2018): 4494.

2. **Wang, Junchao**, Kaining Han, Anastasios Alexandridis, Zeljko Zilic, Yu Pang, Wei Wu, Sadia Din, and Gwanggil Jeon. "A novel security scheme for Body Area Networks compatible with smart vehicles." Computer Networks 143 (2018): 74-81.

3. **Wang, Junchao**, Kaining Han, Anastasios Alexandridis, Zeljko Zilic, Jinzhao Lin, Yu Pang, and Xiaomin Yang. "A baseband processing ASIC for body area networks." Journal of Ambient Intelligence and Humanized Computing (2018): 1-8.

4. **Wang, Junchao**, Wei Wu, Kaining Han, Anastasios Alexandridis, Zhiyu Chen, Zeljko Zilic, Yu Pang, Jinzhao Lin, and Gwanggil Jeon. "A Blockchain-Based eHealthcare System Interoperating with Wireless Body Area Networks." Applied Sciences (Under Review)

5. Han, Kaining, **Junchao Wang**, Warren J Gross, and Jianhao Hu. "Stochastic Bit-Wise Iterative Decoding of Polar Codes." IEEE Transactions on Signal Processing 67.5 (2019): 1138-1151.

6. Pang, Yu, Yafeng Yan, **Junchao Wang**, Zhilong He, and Ting Liu. "Using Arithmetic Transform to Calculate Ranges of Arithmetic Datapaths." JOURNAL OF COMPUTERS 7, no. 12 (2012): 2907.

7. Pang, Yu, Zhi-Long He, Shao-Quan Wang, **Jun-chao Wang**, Xiang Gao, and

Wei Wu. "Efficient methods of range and precision analysis for IIR filters." Dianzi Xuebao(Acta Electronica Sinica) 40, no. 9 (2012): 1752-1758.

***B. Book Chapters:***

8. Liangguang Peng, Jinzhao Lin, Tong Bai, Yu Pang, Guoquan Li, Huiquan Wang, Xiaoming Jiang, **Junchao Wang**, Zeljko Zilic. "An Encryption Method for BAN Using the Channel Characteristics" Advances in Body Area Networks I. Springer, Cham, 2019. 221-233.

***C. Conferences:***

9. **Wang, Junchao**, Kaining Han, Anastasios Alexandridis, Zeljko Zilic, Yu Pang, and Jinzhao Lin. "An ASIC Implementation of Security Scheme for Body Area Networks." In Circuits and Systems (ISCAS), 2018 IEEE International Symposium on, pp. 1-5. IEEE, 2018.

10. **Wang, Junchao**, Kaining Han, Anastasios Alexandridis, Zeljko Zilic, Tong Bai, Jinzhao Lin, Yu Pang, and Guoquan Li. "Using the Characteristic Value of the Body Channel for Encryption of Body Area Networks." In 2018 16th IEEE International New Circuits and Systems Conference (NEWCAS), pp. 265-268. IEEE, 2018.

11. **Wang, Junchao**, Zeljko Zilic, and Yutian Shu. "Evaluation of an RF wearable device for non-invasive real-time hydration monitoring." In Wearable and Implantable Body Sensor Networks (BSN), 2017 IEEE 14th International Conference on, pp. 91-94. IEEE, 2017.

12. **Wang, Junchao**, and Ken Choi. "A carry look-ahead adder designed by reversible logic." In SoC Design Conference (ISOCC), 2014 International, pp. 216-217. IEEE, 2014.

13. **Wang, Junchao**, Yu Pang, and Yang Xia. "A BCD priority encoder designed by reversible logic." In Wavelet Active Media Technology and Information Processing (ICWAMTIP), 2012 International Conference on, pp. 318-321. IEEE, 2012.

14. Chen, Zhiyu, **Junchao Wang**, Kaining Han, and Zeljko Zilic. "Software Defined Radio-Based Testbed for Wireless Body Area Network." In 2018 IEEE 18th International Conference on Bioinformatics and Bioengineering (BIBE), pp. 221-224. IEEE, 2018.

15. Bai, Tong, Jinzhao Lin, Yu Pang, Guoquan Li, Zhangyong Li, Huiqian Wang, **Junchao Wang**, and Zeljko Zilic. "Protocol with self-adaptive GB for WBANs." IET Communications 12, no. 9 (2018): 1042-1047.

16. Pang, Yu, **Junchao Wang**, and Shaoquan Wang. "A 16-bit carry skip adder designed by reversible logic." In Biomedical Engineering and Informatics (BMEI), 2012 5th International Conference on, pp. 1332-1335. IEEE, 2012.

17. Liu, Jing, Jin-zhao Lin, **Jun-chao Wang**, and Yu Pang. "Design of CNFET full adder with mirror structure." In Wireless Communication and Sensor Network: Proceedings of the International Conference on Wireless Communication and Sensor Network (WCSN 2015), pp. 1019-1024. 2016.

18. Qian, Junzhou, and **Junchao Wang**. "A 4-bit array multiplier design by reversible logic." In Information Technology: Proceedings of the 2014 International Symposium on Information Technology (ISIT 2014), Dalian, China, 14-16 October 2014, p. 5. CRC Press, 2015.

References

[1] WHO — Address to the Sixty-ninth World Health Assembly, 2016.

[2] Lara J Akinbami and Jeanne E Moorman. Asthma Prevalence, Health Care Use, and Mortality: United States. Technical report, 2005.

[3] M Ambigavathi and D Sridharan. Energy efficient and load balanced priority queue algorithm for Wireless Body Area Network. *Future Generation Computer Systems*, 11 2018.

[4] Adrian Antipa, Daniel Brown, Alfred Menezes, René Struik, and Scott Vanstone. Validation of Elliptic Curve Public Keys. pages 211–223. Springer, Berlin, Heidelberg, 2003.

[5] Stefan Aust, R Venkatesha Prasad, and Ignas G M M Niemegeers. Advances in Wireless M2M and IoT: Rapid SDR-prototyping of IEEE 802.11ah. In *In the Proceedings of the 39th IEEE Conference on Local Computer Networks (LCN), Demo Abstract*, pages 1–3, 2014.

[6] Ayan Banerjee, K Venkatasubramanian, and Sandeep K S Gupta. Challenges of implementing cyber-physical security solutions in body area networks. In *Proceedings of the Fourth International Conference on Body Area Networks*, page 18, 2009.

[7] Deena M. Barakah and Muhammad Ammad-uddin. A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of a Virtual Doctor Server in Existing Architecture. In *2012 Third International Conference on Intelligent Systems Modelling and Simulation*, pages 214–219. IEEE, 2 2012.

[8] E Barker, W Barker, W P Burr, and M Smid. NIST SP800-57 Recommendation for Key Management, Part 1: General. *Retrieved September*, 5(2009):800–857, 2007.

[9] Elaine B Barker, Don Johnson, and Miles E Smid. *Recommendation for Pair-wise Key Establishment Schemes Using Discrete Logarithm Cryptography:(revised)*. National Institute of Standards and Technology, 2007.

[10] Bacchus Barua. Waiting Your Turn: Wait Times for Health Care in Canada, 2017 Report. Technical report, 2016.

[11] M Barua, M S Alam, Xiaohui Liang, and Xuemin Shen. Secure and quality of service assurance scheduling scheme for WBAN with application to eHealth. In *2011 IEEE Wireless Communications and Networking Conference*, pages 1102–1106. IEEE, 11 2011.

[12] Daniel J. Bernstein. Curve25519: New Diffie-Hellman Speed Records. pages 207–228. Springer, Berlin, Heidelberg, 2006.

[13] Ian Blake, Gadiel Seroussi, and Nigel Smart. *Elliptic curves in cryptography*, volume 265. Cambridge university press, 1999.

[14] Søren Brage, Niels Brage, P W Franks, U Ekelund, and N J Wareham. Reliability and validity of the combined heart rate and movement sensor Actiheart. *European journal of clinical nutrition*, 59(4):561, 2005.

[15] Lindsay Brown, Jef van de Molengraft, Refet Firat Yazicioglu, Tom Torfs, Julien Penders, and Chris Van Hoof. A low-power, wireless, 8-channel EEG monitoring headset. In *2010 Annual International Conference of the IEEE Engineering in Medicine and Biology*, pages 4197–4200. IEEE, 8 2010.

[16] Christopher Byrne and Chin Leong Lim. The ingestible telemetric body core temperature sensor: a review of validity and exercise applications. *British journal of sports medicine*, 41(3):126–33, 3 2007.

[17] Canadian Institute for Health Information. National Health Expenditure Trends, 1975 to 2017. Technical report, Ottawa, ON, 2017.

[18] Haowen Chan, Adrian Perrig, and Dawn Song. Random key predistribution schemes for sensor networks. In *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, pages 197–213, 2003.

[19] Margaret Chan. Address to the Sixty-fifth World Health Assembly. *See http://www. who. int/dg/speeches/2016/wha-69/en/(accessed 26 May 2016)*, 2016.

[20] D Chase. Class of algorithms for decoding block codes with channel measurement information. *IEEE Transactions on Information Theory*, 18(1):170–182, 11 1972.

[21] Mengyuan Chen, Jun Han, Dabin Fang, Yao Zou, and Xiaoyang Zeng. An ultra low-power and area-efficient baseband processor for WBAN transmitter. In *Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2013 Asia-Pacific*, pages 1–4, 2013.

[22] Yu M. Chi and Gert Cauwenberghs. Wireless Non-contact EEG/ECG Electrodes for Body Sensor Networks. In *2010 International Conference on Body Sensor Networks*, pages 297–301. IEEE, 6 2010.

[23] Houcine Chougrani, Jean Schwoerer, Pierre-Henri Horren, Amer Baghdadi, and Francois Dehmas. UWB-IR digital baseband architecture for IEEE 802.15. 6 wireless BAN. In *Electronics, Circuits and Systems (ICECS), 2014 21st IEEE International Conference on*, pages 866–869, 2014.

[24] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things, 2016.

[25] Mauro Conti, Ali Dehghantanha, Katrin Franke, and Steve Watson. Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78:544–546, 11 2018.

[26] Dave Cooper. Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile. 2008.

[27] Oscar Delgado-Mohatar, Amparo Fúster-Sabater, and José M Sierra. A lightweight authentication scheme for wireless sensor networks. *Ad Hoc Networks*, 9(5):727–735, 11 2011.

[28] Chad R Dougherty. Vulnerability Note VU# 836068 MD5 vulnerable to collision attacks. *Retrieved August*, 26:2009, 2009.

[29] Morris Dworkin. Recommendation for block cipher modes of operation. methods and techniques. Technical report, NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD COMPUTER SECURITY DIV, 2001.

[30] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.

[31] Y. Fan and Z. Zilic. BER Testing of Communication Interfaces. *IEEE Transactions on Instrumentation and Measurement*, 57(5):897–906, 5 2008.

[32] G Forney. Generalized minimum distance decoding. *IEEE Transactions on Information Theory*, 12(2):125–131, 11 1966.

[33] Zhangjie Fu, Kui Ren, Jiangang Shu, Xingming Sun, and Fengxiao Huang. Enabling personalized search over encrypted outsourced data with efficiency improvement. *IEEE transactions on parallel and distributed systems*, 27(9):2546–2559, 2016.

[34] H. Fukushima, H. Kawanaka, M. S. Bhuiyan, and K. Oguri. Estimating heart rate using wrist-type Photoplethysmography and acceleration sensor while running. In *2012 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 2901–2904. IEEE, 8 2012.

[35] Robert Gallant, Robert Lambert, and Scott Vanstone. Improving the parallelized Pollard lambda search on anomalous binary curves. *Mathematics of Computation of the American Mathematical Society*, 69(232):1699–1705, 2000.

[36] Carles Gomez, Joaquim Oller, and Josep Paradells. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors*, 12(9):11734–11753, 2012.

[37] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645–1660, 11 2013.

[38] Kaining Han, Junchao Wang, and Warren J Gross. Stochastic Computing based BCH Decoder for WBAN Systems. In *Midwest Circuits and Systems Conference (MWSCAS), 2018 IEEE 61st International*, page in press, 2018.

[39] Michael Helmling and S Scholl. Database of channel codes and ml simulation results. *www. uni-kl. de/channel-codes, University of Kaiserslautern*, 2016.

[40] Romain Heloir, Camille Leroux, Saied Hemati, Matthieu Arzel, and Warren J Gross. Stochastic chase decoder for Reed-Solomon codes. In *New Circuits and*

*Systems Conference (NEWCAS), 2012 IEEE 10th International*, pages 5–8, 2012.

[41] Ilias Iakovidis. Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe 1. *International Journal of Medical Informatics*, 52:105–115, 1998.

[42] Institute of Electrical, Electronics Engineers., and IEEE-SA Standards Board. *IEEE standard for local and metropolitan area networks. Part 15.6, Wireless body area networks*. Institute of Electrical and Electronics Engineers, 2012.

[43] J.L. Jacobs, P. Embree, M. Glei, S. Christensen, and P.K. Sullivan. Characterization of a novel heart and respiratory rate sensor. In *The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, volume 3, pages 2223–2226. IEEE.

[44] L V Jian. Improvement of hierarhical diagnosis and treatment system under deepening medical and health reform. *Chinese Hospital Management*, 34(6):1–3, 2014.

[45] Boseok Jung, Taesung Kim, and Hanho Lee. Low-Complexity Non-Iterative Soft-Decision BCH Decoder Architecture for WBAN Applications. *JOURNAL OF SEMICONDUCTOR TECHNOLOGY AND SCIENCE*, 16(4):488–496, 2016.

[46] Kevin G Kinsella and David R Phillips. *Global aging: The challenge of success*, volume 60. Population Reference Bureau Washington, DC, 2005.

[47] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[48] Neal Koblitz. CM-Curves with Good Cryptographic Properties. In *Crypto*, volume 91, pages 279–287, 1991.

[49] Hugo Krawczyk, Mihir Bellare, and Ran Canetti. RFC 2104: HMAC: Keyed-hashing for message authentication. 1997.

[50] Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6):1211–1220, 11 2017.

[51] Kyung Sup Kwak, Sana Ullah, and Niamat Ullah. An overview of IEEE 802.15. 6 standard. In *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on*, pages 1–6, 2010.

[52] Ohhwan Kwon, Jinwoo Jeong, Hyung Bin Kim, In Ho Kwon, Song Yi Park, Ji Eun Kim, and Yuri Choi. Electrocardiogram Sampling Frequency Range Acceptable for Heart Rate Variability Analysis. *Healthcare informatics research*, 24(3):198–206, 7 2018.

[53] Camille Leroux, Saied Hemati, Shie Mannor, and Warren J Gross. Stochastic chase decoding of Reed-Solomon codes. *IEEE Communications Letters*, 14(9):863–865, 2010.

[54] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. A survey on the security of blockchain systems. *Future Generation Computer Systems*, 11 2017.

[55] X Liang, C Zhang, M Xu, S Zhang, and X You. Efficient stochastic list successive cancellation decoder for polar codes. In *Proc. 28th IEEE Int. System-on-Chip Conf. (SOCC)*, pages 421–426, 11 2015.

[56] Shinyoung Lim, Tae Hwan Oh, Young B Choi, and Tamil Lakshman. Security issues on wireless body area network for remote healthcare monitoring. In *Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on*, pages 327–332, 2010.

[57] Kai Lin, Wenjian Wang, Xianbin Wang, Wen Ji, and Jiafu Wan. QoE-driven spectrum assignment for 5G wireless networks using SDR. *IEEE Wireless Communications*, 22(6):48–55, 11 2015.

[58] Y M Lin, H C Chang, and C Y Lee. Improved High Code-Rate Soft BCH Decoder Architectures With One Extra Error Compensation. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 21(11):2160–2164, 11 2013.

[59] Xin Liu, Yuanjin Zheng, Bin Zhao, Yisheng Wang, and Myint Wai Phyu. An Ultra Low Power Baseband Transceiver IC for Wireless Body Area Network in 0.18um CMOS Technology. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 19(8):1418–1428, 2011.

[60] Vikash Mainanwal, Mansi Gupta, and Shravan Kumar Upadhayay. A survey on wireless body area network: Security technology and its design methodology issue. In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pages 1–5. IEEE, 11 2015.

[61] H. Mamaghanian, N. Khaled, D. Atienza, and P. Vandergheynst. Compressed Sensing for Real-Time Energy-Efficient ECG Compression on Wireless Body Sensor Nodes. *IEEE Transactions on Biomedical Engineering*, 58(9):2456–2466, 9 2011.

[62] Priya Mathew, Lismi Augustine, Deepak Kushwaha, Vivian Desalphine, and A David Selvakumar. Implementation of NB PHY transceiver of IEEE 802.15. 6 WBAN on FPGA. In *VLSI Systems, Architecture, Technology and Applications (VLSI-SATA), 2015 International Conference on*, pages 1–6, 2015.

[63] Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 417–426, 1985.

[64] Peter L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–243, 1 1987.

[65] Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith, and Abbas Jamalipour. Wireless Body Area Networks: A Survey. *IEEE Communications Surveys & Tutorials*, 16(3):1658–1686, 11 2014.

[66] A Naderi, S Mannor, M Sawan, and W J Gross. Delayed Stochastic Decoding of LDPC Codes. *IEEE Transactions on Signal Processing*, 59(11):5617–5626, 11 2011.

[67] R Naseer and J Draper. Parallel double error correcting code design to mitigate multi-bit upsets in SRAMs. In *Proc. ESSCIRC 2008 - 34th European Solid-State Circuits Conf*, pages 222–225, 11 2008.

[68] Gerald Osband. Blockchain: The Concept for Health Plan CMOs.

[69] Sanjana Panicker, Vaishnavi Patil, Divya Kulkarni, and B E Student. I nternational J ournal of I nnovative R esearch in S cience, E ngineering and T echnology An Overview of Blockchain Architecture and it's Applications. *Certified Organization)*, 3297(11), 2007.

[70] I Perez-Andrade, S Zhong, R G Maunder, B M Al-Hashimi, and L Hanzo. Stochastic Computing Improves the Timing-Error Tolerance and Latency of

Turbo Decoders: Design Guidelines and Tradeoffs. *IEEE Access*, 4:1008–1038, 2016.

[71] John M Pollard. Monte Carlo methods for index computation. *Mathematics of computation*, 32(143):918–924, 1978.

[72] Sofia Najwa Ramli, Rabiah Ahmad, Mohd Faizal Abdollah, and Eryk Dutkiewicz. A biometric-based security for data authentication in wireless body area network (wban). In *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, pages 998–1001, 2013.

[73] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, 88:173–190, 11 2018.

[74] M N O Sadiku and C M Akujuobi. Software-defined radio: a brief overview. *IEEE Potentials*, 23(4):14–15, 11 2004.

[75] Pascal Sasdrich and Tim Güneysu. Implementing Curve25519 for Side-Channel–Protected Elliptic Curve Cryptography. *ACM Transactions on Reconfigurable Technology and Systems*, 9(1):1–15, 11 2015.

[76] Roel Schiphorst, Fokke Hoeksema, and Kees Slump. Bluetooth demodulation algorithms and their performance. In *2nd Karlsruhe Workshop on Software Radios*, pages 99–106, 2002.

[77] Georgios Selimis, Li Huang, Fabien Massé, Ioanna Tsekoura, Maryam Ashouei, Francky Catthoor, Jos Huisken, Jan Stuyt, Guido Dolmans, Julien Penders, and others. A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design. *Journal of medical systems*, 35(5):1289–1298, 2011.

[78] Kimia Shamaei, Joe Khalife, and Zaher M Kassas. Performance Characterization of Positioning in LTE Systems. In *In Proceedings of ION GNSS Conference*, pages 2262–2270, 2016.

[79] Jian Shen, Shaohua Chang, Jun Shen, Qi Liu, and Xingming Sun. A lightweight multi-layer authentication protocol for wireless body area networks. *Future Generation Computer Systems*, 78:956–963, 11 2018.

[80] Lu Shi, Ming Li, Shucheng Yu, and Jiawei Yuan. BANA: Body Area Network Authentication Exploiting Channel Characteristics. *IEEE Journal on Selected Areas in Communications*, 31(9):1803–1816, 11 2013.

[81] Alexandru Soceanu, Maksym Vasylenko, Alexandru Egner, and Traian Muntean. Managing the Privacy and Security of eHealth Data. In *2015 20th International Conference on Control Systems and Computer Science*, pages 439–446. IEEE, 11 2015.

[82] Economist Staff. Blockchains: The great chain of being sure about things. *The Economist. Retrieved*, 18, 2016.

[83] Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, and Yarik Markov. The first collision for full SHA-1. *IACR Cryptology ePrint Archive*, 2017:190, 2017.

[84] Thomas J Sullivan, Stephen R Deiss, and Gert Cauwenberghs. A Low-Noise, Non-Contact EEG/ECG Sensor. In *2007 IEEE Biomedical Circuits and Systems Conference*, pages 154–157. IEEE, 11 2007.

[85] Melanie Swan. *Blockchain : blueprint for a new economy.*

[86] Steven A. Taylor and Hamid Sharif. Wearable Patient Monitoring Application (ECG) using Wireless Sensor Networks. In *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 5977–5980. IEEE, 8 2006.

[87] S Sharifi Tehrani, S Mannor, and W J Gross. Fully Parallel Stochastic LDPC Decoders. *IEEE Transactions on Signal Processing*, 56(11):5692–5703, 11 2008.

[88] Parth Thakkar, Senthil Nathan, and Balaji Vishwanathan. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform. 11 2018.

[89] Sana Ullah, Manar Mohaisen, and Mohammed A Alnuem. A review of IEEE 802.15. 6 MAC, PHY, and security specifications. *International Journal of Distributed Sensor Networks*, 9(4):950704, 2013.

[90] US patent: US5165407A. Implantable glucose sensor, 4 1991.

[91] US patent: US5640964A. Wrist mounted blood pressure sensor, 2 1995.

[92] US Patent: US6533729B1. Optical noninvasive blood pressure sensor and method, 5 2000.

[93] US patent: US6629776B2. Digital sensor for miniature medical thermometer, and body temperature monitor, 12 2001.

[94] US patent: US6815186B2. Implantable glucose sensor, 1 2002.

[95] US patent: US7134999B2. Optimized sensor geometry for an implantable glucose sensor, 8 2003.

[96] US patent: US7674231B2. Wearable pulse wave velocity blood pressure sensor and methods of calibration thereof, 8 2007.

[97] A Vardy and Y Be'ery. Maximum-likelihood soft decision decoding of BCH codes. *IEEE Transactions on Information Theory*, 40(2):546–554, 11 1994.

[98] A. Vaz, A. Ubarretxena, I. Zalbide, D. Pardo, H. Solar, A. Garcia-Alonso, and R. Berenguer. Full Passive UHF Tag With a Temperature Sensor Suitable for Human Body Temperature Monitoring. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 57(2):95–99, 2 2010.

[99] David Wagner. A generalized birthday problem. In *Annual International Cryptology Conference*, pages 288–304, 2002.

[100] J Wang, K Han, A Alexandridis, Z Zilic, Y Pang, W Wu, S Din, and G Jeon. A novel security scheme for Body Area Networks compatible with smart vehicles. *Computer Networks*, 143, 2018.

[101] Junchao Wang, Kaining Han, Anastasios Alexandridis, Zeljko Zilic, Jinzhao Lin, Yu Pang, and Xiaomin Yang. A baseband processing ASIC for body area networks. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–8, 11 2018.

[102] Junchao Wang, Kaining Han, Anastasios Alexandridis, Zeljko Zilic, Yu Pang, and Jinzhao Lin. An ASIC Implementation of Security Scheme for Body Area Networks. In *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–5. IEEE, 11 2018.

[103] Junchao Wang, Kaining Han, Zhiyu Chen, Anastasios Alexandridis, Zeljko Zilic, Yu Pang, Jinzhao Lin, Junchao Wang, Kaining Han, Zhiyu Chen, Anastasios Alexandridis, Zeljko Zilic, Yu Pang, and Jinzhao Lin. A Software Defined Radio Evaluation Platform for WBAN Systems. *Sensors*, 18(12):4494, 12 2018.

[104] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. CRC press, 2008.

[105] Stephen B Wicker. *Error control systems for digital communication and storage*, volume 1. Prentice hall Englewood Cliffs, 1995.

[106] Michael J Wiener and Robert J Zuccherato. Faster attacks on elliptic curve cryptosystems. In *Selected areas in Cryptography*, volume 1556, pages 190–200, 1998.

[107] Z Xie, S Dai, H-N Chen, and X Wang. Blockchain challenges and opportunities: a survey. Technical Report 4, 2018.

[108] Xiong Xiong, Wei Xiang, Kan Zheng, Hengyang Shen, and Xingguang Wei. An open source SDR-based NOMA system for 5G networks. *IEEE Wireless Communications*, 22(6):24–32, 12 2015.

[109] W Xueqiang, P Liyang, W Dong, H Chaohong, and Z Runde. A High-Speed Two-Cell BCH Decoder for Error Correcting in MLC nor Flash Memories. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 56(11):865–869, 11 2009.

[110] C H Yang, T Y Huang, M R Li, and Y L Ueng. A 5.4 \mu{\rm W}Soft-Decision BCH Decoder for Wireless Body Area Networks. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 61(9):2721–2729, 9 2014.

[111] B Yuan and K K Parhi. Belief propagation decoding of polar codes using stochastic computing. In *Proc. IEEE Int. Symp. Circuits and Systems (ISCAS)*, pages 157–160, 11 2016.

[112] Hiromi Yuasa, Hideaki Fukuzawa, Yoshihiko Fuji, Alexander Devin Giddings, Michiko Hara, and Shuichi Murakami. Blood-pressure sensor. *US Patent App. 13/045,759*, 12 2011.

[113] Chris F. Zhang and Tae-Wuk Bae. VLSI Friendly ECG QRS Complex Detector for Body Sensor Networks. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 2(1):52–59, 3 2012.

[114] Jie Zhang, Nian Xue, and Xin Huang. A Secure System for Pervasive Social Network-Based Healthcare. *IEEE Access*, 2016.

[115] Y.J. Zhao, A. Davidson, J. Bain, S.Q. Li, Q. Wang, and Q. Lin. A MEMS viscometric glucose monitoring device. In *The 13th International Conference on Solid-State Sensors, Actuators and Microsystems, 2005. Digest of Technical Papers. TRANSDUCERS '05.*, volume 2, pages 1816–1819. IEEE.

[116] Zhaoyang Zhang, Honggang Wang, A V Vasilakos, and Hua Fang. ECG-Cryptography and Authentication in Body Area Networks. *IEEE Transactions on Information Technology in Biomedicine*, 16(6):1070–1078, 11 2012.

[117] Cong-Xu Zhu, Yu-Ping Hu, and Ke-Hui Sun. New image encryption algorithm based on hyperchaotic system and ciphertext diffusion in crisscross pattern. *Dianzi Yu Xinxi Xuebao(Journal of Electronics and Information Technology)*, 34(7):1735–1743, 2012.

[118] Tanveer A Zia and Albert Y Zomaya. A Lightweight Security Framework for Wireless Sensor Networks. *JoWUA*, 2(3):53–73, 2011.

[119] Howard Zisser, Lauren Robinson, Wendy Bevier, Eyal Dassau, Christian Ellingsen, Francis J Doyle III, and Lois Jovanovic. Bolus calculator: a review of four "smart" insulin pumps. *Diabetes technology & therapeutics*, 10(6):441–444, 2008.

[120] Dimitrios Zissis and Dimitrios Lekkas. Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3):583–592, 11 2012.

[121] A.J. Zuckerwar, R.A. Pretlow, J.W. Stoughton, and D.A. Baker. Development of a piezopolymer pressure sensor for a portable fetal heart rate monitor. *IEEE Transactions on Biomedical Engineering*, 40(9):963–969, 1993.

[122] Guy Zyskind, Oz Nathan, and Alex 'Sandy' Pentland. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184. IEEE, 11 2015.