SECURE AND EFFICIENT CERTIFICATELESS SIGNCRYPTION PROTOCOL FOR WIRELESS BODY AREA NETWORKS

MISHECK MURIMI KING'ANG'I

A Thesis Submitted to Graduate School in Partial Fulfillment for the Requirement for the Award of Degree of Master of Science in Computer Science of Tharaka University.

THARAKA UNIVERSITY

NOVEMBER 2024

DECLARATION AND RECOMMENDATION

Declaration

This thesis is my original work and has not been presented for an award of a diploma or conferment of degree in any institution.

Signature.....Date.....20/11/2024.....

Misheck Murimi King'ang'i
SMT22/03130/20

Recommendation

This thesis has been submitted for examination with our approval as University supervisors.

Signature.....Date.....20/11/2024.....

Dr. Ismael M. Kwenga, PhD
Tharaka University

Signature.....Date.....22/11/2024.....

Mr. Daniel Mukathe, MEng
Tharaka University

i

DEDICATION

Every success of a challenging work requires self-effort and support from people who are close to our hearts. I therefore dedicate this thesis to my beloved wife, Caroline, whose unwavering support and encouragement have been my constant source of strength. To my wonderful daughters, Joyleen and Velma, your love and smiles have been a beacon of inspiration throughout this journey. To my mother, Hellen Kathuure, whose wisdom, prayers, and sacrifices have laid the foundation for my success, I owe you my deepest gratitude. To my siblings, James, Shadrack, and Rosemary, your camaraderie and belief in me have been invaluable. Lastly, to my nephew, Ephantus, and my nieces, Moreen, Lizbeth, and Tiffany, your joy and enthusiasm have been a source of great motivation. This work is a testament to the love, dedication, and support of my family, to whom I am eternally grateful.

ACKNOWLEDGEMENT

First, I express my heartfelt gratitude to the Almighty God for His unwavering love, care, and protection that have guided me throughout this incredible journey. Next, I extend my most profound appreciation to my esteemed supervisors, Dr. Ismael Kwenga and Mr. Daniel Mukathe for their invaluable contributions, insightful comments, remarkable guidance, and selfless commitment throughout the research process. Special appreciation goes to Mr. John Majira for his daily encouragement during this journey. Furthermore, let me thank my lecturers, classmates, workmates, and the entire Tharaka University for providing an enabling environment to carry out my research. Finally, I convey my special regards to my wife and the whole family for being supportive all along. Their effort can't go unnoticed.

ABSTRACT

The Wireless Body Area Networks (WBAN) are healthcare systems that provides timely remote health monitoring for patients. It involves wearable biosensors that collect, aggregate, and transmit physiological data to a medical server for automatic diagnosis and treatment. However, WBAN entities communicate via wireless IEEE 802.15.6, an insecure short-range communication standard. Therefore, this exposes patients' sensitive data to confidentiality, privacy, and authentication security breaches. Additionally, WBAN entities are resource-constrained devices that demand lightweight computational algorithms. Meanwhile, researchers have designed numerous schemes to combat the above-mentioned breaches. Nevertheless, many existing schemes are based on bilinear pairing and certificate management, which entail heavy cryptographic operations. Thus, this subjects them to communication and computational inefficiencies. To resolve these problems, this study utilized certificateless bilinear-pairing-free elliptic curve cryptography and general hash functions to design and validate a secure and efficient signcryption scheme for signcrypting and unsigncrypting messages. The study utilized primary and secondary data regarding the running time for cryptographic operations in the proposed scheme and other related schemes respectively. To generate the running times for the various cryptographic operations considered, the study utilized the Mult-precision Integer and Rational Arithmetic Cryptographic Library for C/C++ (MIRACL CC) toolkit. Besides, the study conducted formal security proof using the Random Oracle Model (ROM) to demonstrate Indistinguishability under a Chosen Ciphertext Attack (IND-CCA) and Existential Unforgeability under a Chosen Message Attack (EUF-CMA) and informal analysis to illustrate the scheme's resilience for typical attacks, such as impersonation attacks, replay attacks, man-in-the-middle attacks, and modification attacks. From the formal security proof, the proposed scheme has proven to be IND-CCA and EUF-CMA secure against adversaries of Type I and Type II. Regarding performance analysis, the study analyzed the computational and communication costs and compared them with state-of-the-art works, where the proposed scheme showed computation efficiency improvements of 94.65%, 68.46%, 96.69%, 52,55%, 93.99%, and 40.03% against schemes in Xiong et al., Zhou, Liu et al., Ullah et al., Ramadan et al., and Zhang et al., respectively, and a communication efficiency improvement of 76.27%, 71.72%, 59.71%, and 8.93% against schemes in Xiong et al., Liu et al., Ramadan et al., and Zhang et al., respectively. On the other hand, the study conducted an experiment to evaluate end-to-end delay, throughput, and packet loss ratio through network simulation using the NS-3 platform, and the proposed scheme outperformed other similar schemes in terms of network performance by attaining the highest throughput of up to 900 messages when 5 PDs are deployed, a steady and lowest latency of 43.7 ms for end-to-end delay, and the lowest packet loss ratio of 12.4%, according to the simulation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

AP	Application Provider
BLE	Bluetooth Low Energy
CLC	Certificateless Cryptography
DoS	Denial of Service
ECC	Elliptic Curve Cryptography
ECDHP	Elliptic Curve Diffie-Hellman Problem
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECG	Electrocardiogram
EUF-CMA	Existentially Unforgeable under adaptive Chosen Message Attack
IND-CCA	Indistinguishability under Chosen Ciphertext Attack
IBC	Identity Based Cryptography
IoT	Internet of Things
MAC	Medium Access Control
MIRACL	Mult-precision Integer and Rational Arithmetic Cryptographic Library
MITM	Man-In-The Middle
NACOSTI	National Commission for Science, Technology and Innovations
NM	Network Manager
NS-3	Network Simulator 3
PD	Patient's Device
PFS	Perfect Forward Secrecy
PID	Pseudo Identity
PKC	Public Key Cryptography
PKE	Public Key Encryption
PKI	Public Key Infrastructure
QKD	Quantum Key Distribution
QoS	Quality of Service
RID	Real Identity
ROM	Random Oracle Model
RSA	Rivest Shamir Adleman
RSS	Received Signal Strength
TA	Trusted Authority
WBAN	Wireless Body Area Network
XOR	Exclusive OR

CHAPTER ONE
INTRODUCTION

1.1. Background of the Study

The remarkable progress of the Internet of Things (IoT) in the recent past has led to the rise of the wireless body area networks (WBANs), a cutting-edge healthcare system that enables the monitoring of patients' health conditions without the need for continuous physician supervision and aids in the diagnosis of diseases.

WBAN refers to a wireless network involving the human body, biosensors, application provider, and network manager, as depicted in Figure 1.1 (Mandal, 2022; Teshome et al., 2018). The human body avails physiological data (i.e., body temperature, blood pressure, heart rate, blood sugar level, and Electrocardiogram (ECG)) to biosensors implanted inside or outside the human body. Upon receiving physiological data, the biosensors transmit the data to the application provider for immediate diagnosis and treatment.

In addition, WBAN contains an aggregator, such as a mobile device, which is responsible for collecting and aggregating data from multiple biosensors and transmitting it to the application provider (Almuhaideb, 2022). The network manager acts as a trusted authority mandated for the entire network management, including registration and revocation of entities.

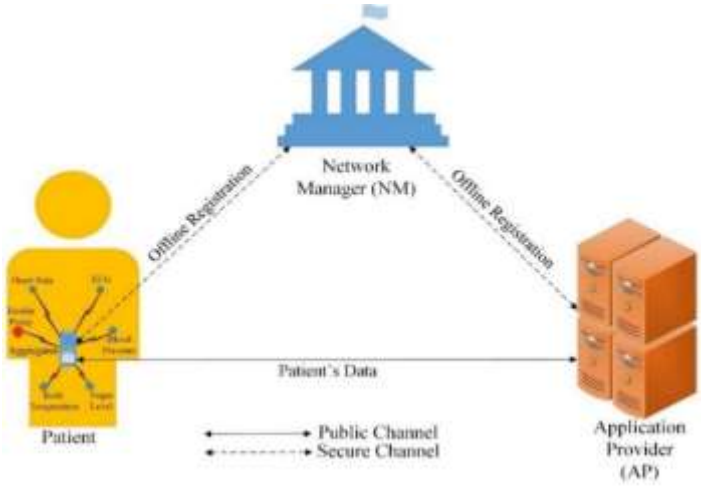

Figure 1.1: WBAN Components

Source: Author

The biosensors connect with the aggregator in a star or multi-hop topology, and their communication occurs via the short-range communication standard called IEEE 802.15.6 (Cornet et al., 2022; Qu et al., 2019). IEEE 802.15.6 offers security for WBAN communication at three levels, depending on the specific security requirements. The first level is level 0, which is characterized by unsecure communication. In this level, data transmission does not include any security measures such as authentication, confidentiality, integrity, or mechanisms to resist replay attacks. This level is therefore unsuitable for WBAN communication. The second level is level 1, which provides typical security by providing an authentication mechanism for communicating devices. It is applicable when the system of communication needs to establish the legitimacy of the communicating devices. However, the level does not provide confidentiality, privacy, or resistance to replay attacks. Finally, the third level is level 2. It is the most secure level for the IEEE 802.15.6 standard, where it provides authentication and encryption features together, thus solving all the problems associated with levels 0 and 1. This makes it ideal for the WBAN environment, which requires confidentiality of patients' data. This study therefore adopts the IEEE 802.15.6 level 2 standard to design a secure communication protocol for WBANs.

WBAN provides numerous benefits to patients and medical service providers, such as real-time and remote health monitoring of patients' conditions for early detection of abnormalities. For instance, WBANs ensure automated health care for patients with diabetes by detecting the glucose level and stimulating the insulin pump to release insulin, thus providing automatic dosing in diabetics (Jegadeesan et al., 2020). As a result, the patients and medical service providers save time and resources.

Despite the numerous benefits provided by WBANs, the network is coupled with several challenges, some of which are life-threatening. Firstly, data in this network is transmitted through insecure public channels exposing sensitive data to security risks such as message injection, eavesdropping, message replay, spoofing, and compromise to the integrity of the message (Asam et al., 2019). For instance, data may be altered, leading to wrong diagnosis, posing a risk to patient's safety, and potentially leading to catastrophic consequences.

Secondly, the confidentiality of patients' data is required to safeguard against unauthorized access, which could lead to ill purposes such as cybercrimes. Finally, biosensors in WBANs

are resource-constrained due to their tiny size nature, thus limiting their ability to handle highly complex computations while providing efficiency (Mandal, 2022). Therefore, this research was thrilled by the above-mentioned challenges to propose a secure and efficient certificateless signcryption protocol for wireless body area networks.

1.2. Statement of the Problem

The WBAN environment is public and poses significant security and confidentiality risks. For instance, patient health data should remain confidential, and only permitted entities have access. Moreover, the entities communicating in WBAN have limited computing power. Therefore, efficiency is a critical requirement. Several schemes have been proposed to achieve secure communication through an insecure channel. However, many schemes such as those of (Zhang et al., 2021), (Umar et al., 202), (Jegadeesan et al., 2020), (Deng & Shi, 2018), and (Meng, 2019) experience security issues coupled with performance overheads. To achieve security, for instance, a number of authors have used heavy cryptographic operations such as those involving bilinear pairing and certificate management, exposing WBAN resource-constrained devices to complex computations, thus compromising efficiency. On the other hand, several schemes presented to achieve WBAN efficiency are coupled with security issues. For instance, (Shen et al., 2018) have used a lightweight computation mechanism, i.e., certificateless elliptic curve cryprography. However, their scheme fails to meet forward secrecy, an important security feature for WBANs. Likewise, (Almuhaideb, 2022) uses a certificateless elliptic curve cryprography mechanism to achieve security and efficiency for WBANs. However, the double authentication protocol in their scheme reduces efficiency. Regarding security weaknesses, several schemes presented by various authors lack sender authentication, unforgeability, key-escrow resistance, forward secrecy, and conditional anonymity. For instance, in Xiong et al. (2022), the scheme presented does not provide sender authentication, conditional anonymity, and key escrow resistance. Likewise, the scheme in Zhou (2019a) lacks conditional anonymity. In the same manner, the scheme presented by Liu et al. (2020) suffers from lack of sender authentication, unforgeability, forward secrecy, and conditional anonymity. Similarly, the Ramadan et al. (2023) scheme does not provide sender authentication, key-escrow resistance, or conditional anonymity. To sum up, schemes

presented to provide mechanisms for WBANs communication suffer efficiency and security issues, which are critical.

1.3. Objectives

1.3.1. General Objective

The objective of this study was to design and evaluate the performance of a secure and efficient certificateless signcryption protocol for wireless body area networks (WBANs)

1.3.2. Specific Objectives

i. To analyze the existing WBAN signcryption schemes through theoretical techniques to obtain secondary data on security strengths and weaknesses and performance efficiency.
ii. To design a secure and efficient certificateless signcryption protocol for WBANs based on pairing-free elliptic curve cryptography (ECC) and general one-way hash functions.
iii. To validate the security and efficiency of the proposed scheme.

1.4. Research Questions

This study aimed at addressing the following questions.

i. What are the key security and efficiency issues of concern affecting the state-of-the-art WBAN signcryption schemes?
ii. What is the most secure and efficient approach to designing a secure communication protocol for?
iii. How effective is the proposed signcryption scheme in ensuring security and maintaining operational efficiency under various threat models and performance conditions?

1.5. Significance of the Study

The study aimed at developing a secure and efficient signcryption protocol for WBAN. Firstly, achieving this objective ensures the security of patients' sensitive data and improves the quality of care by allowing biosensors to communicate with other entities reliably and efficiently. Secondly, the study equips healthcare professionals with a more reliable system to enhance a comprehensive and timely understanding of patients' health conditions

through real-time monitoring and reliable data collection. Thirdly, continuous and detailed patient health data provided by secure WBAN permits early detection of potential health problems and timely intervention, thus improving patient outcomes. Lastly, the study positively impacted the cost of healthcare by reducing the cost through efficiency provided and ultimately reducing the need for hospital visits and re-admissions. The patients are empowered to actively manage their health by providing access to their health data. Therefore, by presenting a secure and efficient signcryption protocol for WBAN communication, healthcare institutions are able to deliver improved quality of patient care by making informed decisions (i.e., the right diagnosis) based on real-time and accurate data. The overall quality of health care is thus improved.

1.6. Scope

This study focused on developing and testing a secure and efficient communication protocol for WBANs. Specifically, the study designed a protocol for transmitting patient data in applications such as chronic disease management, remote patient monitoring, and emergency medical services.

1.7. Limitations

The study was limited by the fact that since WBANs operate in a dynamic environment, e.g., inside the human body, factors such as mobility, interference and signal attenuation can affect network performance, thus simulating these real-world conditions accurately was challenging due to the limitation of NS-3 simulator. Additionally, the study used MIRACL CC library which depended on the computing environment the study adopted. This environment may be different from what other authors used. Finally, the security evaluation of the study's model relied on the theoretical attack models which may not be the case with real-world WBAN environment, as there could be unique security challenges.

1.8. Assumptions

The following presumptions formed the foundation of this study:

i. The network manager (NM) is fully trusted and cannot be compromised to perform malicious activity on the network.

ii. The patient's device (PD) and application provider (AP) are untrusted and could be compromised.

iii. Communication between the NM and other entities in the network is secure and reliable.

iv. The PD and AP communicate using an unreliable network protocol susceptible to attacks.

v. All entities in the network have synchronized clock systems.

1.9. Definition of Terms

Application provider (AP)	An entity or organization that develops or offers software applications, services, or solutions that leverage the data collected from biosensors or wearable devices in a WBAN for specific healthcare or wellness-related purposes.
Certificateless	A cryptographic primitive that eliminated the reliance on digital certificates and associated certificate authorities (CAs).
Entity	Refers to a component or element that participates in the WBAN network
Lightweight	Efficient and resource-friendly for implementation in resource constrained devices.
Network Manager	A component or entity that acts as a central authority and is responsible for managing the overall operation, configuration, and performance of the WBAN.
Patient's device/Aggregator	A component or device that is worn or carried by the patient to collect and/or aggregate data from multiple biosensors or wearable devices within the WBAN, acting as a central hub or gateway that gathers, processes, and transmits data from various sensors or wearables to a remote receiver or a healthcare system for further analysis or action.
Signcryption	A cryptographic technique that combines the functionalities of digital signatures and encryption to sign and encrypt a message in a single logical step.
Unsigncryption	The process of verifying signature and decrypting an encrypted message using a single logical step.

CHAPTER TWO
LITERATURE REVIEW

2.1. Introduction

This chapter is organized as follows: Section 2.2 covers the theoretical framework of the study. Section 2.3 presents related work. The analysis of existing WBAN authentication schemes, techniques for designing a signcryption scheme, and performance evaluation techniques are provided in sections 2.3.1, 2.3.2, and 2.3.3, respectively.

2.2. Theoretical Framework

2.2.1. Resource Constrained Devices

WBAN devices are wearable or implantable devices or sensors that monitor physiological parameters, collect health-related data, and provide medical assistance in real-time. The devices are characterized by limited computational power, memory, energy, and communication capabilities (Al Barazanchi et al., 2021; Safa et al., 2019). Therefore, designing secure and efficient network protocols, algorithms, and applications for these devices poses unique challenges. Below are critical factors to consider when designing WBAN network protocols:

The first factor is the energy efficiency. Optimizing energy consumption is crucial for WBAN devices to extend battery life and ensure long-term operation. Energy-efficient communication protocols, data compression techniques, and low-power sensing mechanisms are essential to minimize energy consumption while maintaining desired functionalities. The second factor to consider is the computational constraints. Resource-constrained devices may have limited processing capabilities, impacting the complexity of data processing tasks and cryptographic operations. Designing lightweight algorithms and efficient data processing techniques tailored for resource-constrained devices is essential to ensure real-time monitoring and analysis of health-related data. The third factor is memory limitations. WBAN devices often have limited memory capacity, making the local processing and storing of massive volumes of data difficult. Therefore, developing efficient data storage, management techniques and data compression algorithms, are necessary to overcome memory constraints and enable effective data handling on resource-constrained devices. The fourth factor to consider when designing WBAN protocols is the

Communication Range and Bandwidth**.** WBAN devices typically have limited communication ranges, especially when operating in wireless environments with potential interference and signal attenuation. Optimizing communication protocols and designing efficient data transmission mechanisms are important to ensure reliable and low-latency communication within the network, despite the limited communication range and available bandwidth. The fifth and last factor is security and privacy. WBAN network should be designed in such a way as to provide: confidentiality which ensures patient's data is protected from unauthorized access, authentication to ensure all entities in the network are fully authenticated before communicating, conditional anonymity to hide the real identities of entities in the network, traceability to allow for network manager trace the real identity of any entity involved in a dispute, and resistance to common network attacks such as Man-in-the-middle attacks (MITM), denial of service attacks (DoS), etc. Resource-constrained devices in WBANs may face the above-mentioned security and privacy challenges due to their limited computational power and memory. Designing lightweight and efficient security mechanisms such as secure key exchange protocols and lightweight encryption algorithms is essential for safeguarding sensitive health information that is transferred and kept on these devices.

2.2.2. Wireless Communication Standards

Wireless communication standards encompass the protocols, rules, and specifications that govern wireless data transmission and reception between devices. These standards define the modulation, encoding, channel access, error correction methods, and other aspects of wireless communication. In wireless communication, the following standards are useful (Al Barazanchi et al., 2021):

The first standard is the *IEEE 802.15.6* that focuses on WBANs and provides short-range, low power, and high-reliability communication guidelines. It outlines the protocols for WBAN devices' media access control (MAC) and physical layers, taking into account the particular needs of healthcare applications. IEEE 802.15.6 supports various communication modes, including point-to-point, point-to-multipoint, and peer-to-peer. It includes adaptive channel selection, power management, and Quality of Service (QoS) mechanisms. The second standard is the Bluetooth Low Energy (BLE), a low-power wireless communication

protocol for short-range connectivity, usually interconnecting wearable devices with smartphones, tablets, or other gateway devices. Operating in the 2.4 GHz frequency band, BLE provides energy-efficient data transmission and low-latency communication and supports a range of profiles and services relevant to healthcare applications. The third standard is Zigbee. Zigbee is a low-power wireless communication protocol that is based on the IEEE 802.15.4 standard, widely used in WBANs and IoT applications. It operates in the 2.4 GHz or 868/915 MHz frequency bands and provides low data rate communication with low power consumption. Mesh networking, which allows devices to create self-organizing networks and increase communication range, is supported by Zigbee. It offers reliable data transmission and network security features and supports various application profiles suitable for WBAN deployments. The fourth standard is the *Wi-Fi (IEEE 802.11*. Wi-Fi can be utilized in WBANs for data transmission between wearable devices and access points, providing higher data rates and a more extended communication range than other standards. Its primary adoption is in healthcare facilities or home environments where a broader coverage area and higher bandwidth are required for WBAN applications. However, Wi-Fi consumes more power. The fifth standard in wireless communication is the Cellular Networks. WBANs can leverage cellular networks, such as 4G LTE or 5G, for data transmission, offering broader coverage, seamless mobility, and higher bandwidth, enabling long-range communication and connectivity beyond the limited range of local wireless standards. However, cellular transmission is unsuitable for resource-constrained WBAN devices due to their higher power consumption and complexity. Nonetheless, it is helpful for specific applications that require extended coverage or remote monitoring.

2.2.3. Provable Security

Designing a cryptographic scheme relies on providing security proof through mathematical frameworks against computationally bounded attackers (Bellare & Rogaway, 1996). Provable security is a concept in cryptography that aims to provide mathematical guarantees and proofs for the security of cryptographic schemes and protocols. It involves designing cryptographic algorithms and protocols with well-defined security models and proving their security properties based on rigorous mathematical foundations. Provable security entails the following components:

The first component is the Random Oracle Model, an idealized mathematical abstraction used in cryptography to model the behavior of hash functions, formally introduced by (Bellare & Rogaway, 1996). It is a hypothetical black box that provides a unique answer to every question. In this model, a hash function behaves like a random oracle, providing unique and random outputs for each input. When a query is submitted again, the oracle returns results that are comparable. The ROM provides a simulation environment to analyze cryptographic schemes based on the presumption that the hash function is ideal. The second component is the set of security models. Cryptography security models are defined as an adversary that attempts to break a cryptographic scheme using efficient algorithms. The security model provides a formal framework to define the security goals and requirements of cryptographic schemes. It specifies the adversary's capabilities, the desired security properties (e.g., confidentiality, integrity, authentication), and the level of security assurance expected from the cryptographic scheme. A cryptographic scheme is said to hold up to weaker attacks if it can resist powerful adversary attacks. In public-key cryptography, security analysis often entails two models including; Chosen Ciphertext Attack (CCA) and Chosen Message Attack (CMA) (Ali et al., 2021). The third component entails the public key encryption. Public Key Encryption (PKE) is a cryptographic technique developed by Diffie (Diffie, W., 1976) that allows two parties to communicate securely using a public key and a corresponding private key. The private key is kept hidden, but the public key is made public. In order to encrypt a message during communication, the sender frequently gets the recipient's public key from the public directory. On the other hand, the receiver uses her private key to decrypt the received message. The fact that public and private key pairs are not identical but mathematically related ensures that only the receiver can read the message.

The fourth component of a provable security is the hash functions. Hash functions are mathematical operations that result in a fixed-size output (hash value) from an input (message). They are mostly used for data integrity, digital signatures, message authentication and other information security related applications (Tchórzewski & Jakóbik, 2019). Hash functions have a fixed-length output, are one-way, and are resistant to collisions. Hash functions possess a number of properties that make them ideal for generation of signatures, including pre-image resistance, a characteristic that states that,

given a hash value, it should be computationally impossible to obtain the original input data (pre-image), i.e., if $H(z)$ is a hashed value for hash function H, it is hard to find input z that results to $H(z)$. The second property is the second pre-image resistance. According to second pre-image resistance, it should be computationally impossible to identify another input message that yields the same hash value given an input message. For example, given H generates $H(x)$ from input x, it is difficult to find z such that $H(z) = H(x)$. The last property is collision resistance. Collision resistance makes sure that finding two distinct input messages that result in the same hash value is computationally challenging. i.e., given hash function H, it is difficult to find inputs x and z which are distinct such that $H(z) = H(x)$. Examples of Hash Functions include: MD5 (Message Digest Algorithm 5), which is a 128-bit hash value, SHA-1 (Secure Hash Algorithm 1), that produces a 160-bit (20-byte) hash value, and SHA-256 (Secure Hash Algorithm 256-bit), which generated hashes with a length of 256 bits.

2.2.4. Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is a public-key cryptography scheme based on the mathematics of elliptic curves over finite fields. It was developed in 1985 by (Miller, 1985) and (Koblitz, 1987) as an alternative public key cryptosystem to provide a secure and efficient method for key exchange, digital signatures, and encryption. Additionally, ECC has a small key size compared to other cryptographic primitives. For instance, a key size of 313 bits in ECC offers a similar security level to 4096 bits in RSA (Kasyoka, 2022), thus making ECC applicable in extensive areas including, secure communication, digital currencies, and embedded systems. Key concepts in ECC include:

2.2.4.1. Elliptic Curves

An elliptic curve is a mathematical curve, and fundamental building block for ECC defined by an equation of the form $y^2 = x^2 + ax + b$ where a and b are constants and where $a, b \in F_P$ and $4a^3 + 27b^2 \neq 0$. The curve has inherent properties that make it suitable for cryptography, such as being non-linear, computationally challenging to solve for discrete logarithms, and having a group structure.

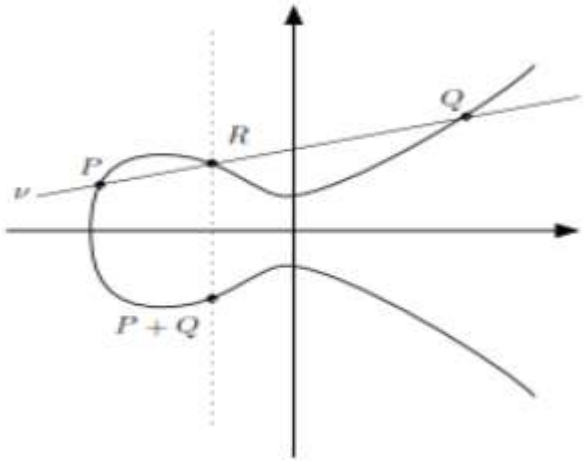

Figure 2.1: Elliptic Curve

Source: (Kasyoka, 2022)

2.2.4.2. Finite Fields

ECC operates over finite fields, which consist of a finite set of elements and supports arithmetic operations like addition, subtraction, multiplication, and division. In ECC, the size of the finite field determines the security level of the cryptographic system.

2.2.4.3. Public and Private Keys

Each user has a pair of keys, i.e., a private key and a public key. The private key is kept secret and used for signing and decryption. The public key is derived from the private key and is made available to others for encryption and verification.

2.2.4.4. Point Addition and Scalar Multiplication

ECC operations are based on point addition and scalar multiplication. Point addition combines two points on the curve to produce a third point. For instance, Taking P, Q as two points on the curve, such that $P + Q = R$, and $-R$ is a third point where the line joining P and Q intersects the curve, then point R is the reflection of $-R$ on x-axis (Mandal, 2022). On the other hand, scalar multiplication involves multiplying a point by an integer (the scalar) to obtain another point on the curve i.e., if point P is a generator of cyclic additive group G. Then, $kP = P + P + \cdots + P(k \text{ times})$ where $k \in \mathbb{Z}_q^*$ (Ali et al., 2021).

2.2.4.5. Computationally Hard Problems

The security of ECC relies on the computational difficulty of solving the discrete logarithm problem, which entails determining the exponent (scalar) when given a base point and the resulting point on the curve, and computational Diffie-Helman Problem (CDHP) which involves computing a third point from two given points as demonstrated below.

Elliptic Curve Discrete Logarithm Problem (ECDLP): Given points $P, Q \in G$, to find an integer $x \in \mathrm{Z}_q^*$ such that $Q = xP$. It is hard to compute x from P and Q by an algorithm that is polynomial time bounded. (Yang et al., 2022).

Computational Diffie-Hellman Problem (CDHP): Given an elliptic curve E defined over a finite field $GF(p)$, a point $P \in E$ of order n, $A = aP,\ B = bP$, it is computationally hard to find to find the point $C = abP$ (Zhang et al., 2021). The problems are believed to be computationally infeasible to solve efficiently. The fundamental mathematical concepts used in the proposed scheme are discussed below:

The first concept is the elliptic curve group. An elliptic curve E over a prime finite field F_P is defined by an equation $y^2 = x^2 + ax + b$ where $a, b \in F_P$ and $4a^3 + 27b^2 \neq 0$. Then $G = \{(x, y): x, y \in F_P, E(x, y) = 0\} \cup \{0\}$ is the additive elliptic curve where O is the point at infinity (Mandal, 2022).

The second concept is Point Addition. Taking P, Q as two points on the curve, such that $P + Q = R$, and $-R$ is a third point where the line joining P and Q intersects the curve, then point R is the reflection of $-R$ on x-axis (Mandal, 2022).

The third concept entails Scalar Multiplication. If point P is a generator of cyclic additive group G. Then, $kP = P + P + \cdots + P(k \text{ times})$ where $k \in \mathbb{Z}_q^*$ (Ali et al., 2021).

The fourth concept is the Elliptic Curve Discrete Logarithm Problem (ECDLP) i.e., given points $P, Q \in G$, to find an integer $x \in \mathrm{Z}_q^*$ such that $Q = xP$. It is hard to compute x from P and Q by an algorithm that is polynomial time bounded. (Yang et al., 2022).

The fifth mathematical concept used in this study is the Computational Diffie-Hellman Problem (CDHP). The concept states that given an elliptic curve E defined over a finite field $GF(p)$, a point $P \in E$ of order n, $A = aP,\ B = bP$, it is computationally hard to find to find the point $C = abP$ (Zhang et al., 2021).

2.2.5. Formal Definition of Signcryption

Signcryption is a cryptographic primitive introduced by (Zheng, 1997) that merges the functionalities of digital signatures and encryption in a single step. It provides confidentiality, integrity, and authenticity for messages, offering efficiency and reduced computational complexity compared to separate signing and encryption operations. The primitive comprises four main algorithms including Setup, Key Generation, Signcryption and Unsigncryption as follows:

$Setup$: $params \longleftarrow \mathcal{R}$: This algorithm requires security parameter $\mathcal{R}$ as the input to generate system parameters $params$

$Key\ Generation$: (SK_S, PK_S) $(SK_R, PK_R) \longleftarrow params$: This algorithm requires system parameters $params$ as the input to generate private-public key pairs of both the sender and receiver.

$Signcryption$: ϱ or $\perp \longleftarrow (params, SK_S, PK_S, PK_R, \mathcal{M})$: This algorithm requires system parameters, private-public key pair of the sender, receiver's public key and message $\mathcal{M}$ as the input to generate ciphertext ϱ or $\perp$.

$Unsigncryption$: $\mathcal{M}'$ or $\perp \longleftarrow (params, SK_R, PK_S, PK_R, \varrho)$: This algorithm requires system parameters, ciphertext ϱ, public key of both the sender and the receiver, and private key of the receiver as the input to generate message $\mathcal{M}'$ or $\perp$.

2.3. Related Work

2.3.1. Analysis of Existing WBAN Authentication Schemes

Researchers have made a remarkable progress in addressing security issues in WBANs by utilizing public key cryptography (PKC) to design various authentication schemes. Based on the PKC technique, the proposed schemes are grouped into public key infrastructure (PKI), identity-based cryptography (IBC), and certificateless cryptography (CLC), as shown in Figure 2.2. The study explains their theoretical concept, indicating whether they are based on elliptic curve cryptography or bilinear pairing. Figure 2.2 summarizes the classification of PKC-based authentication schemes for WBANs.

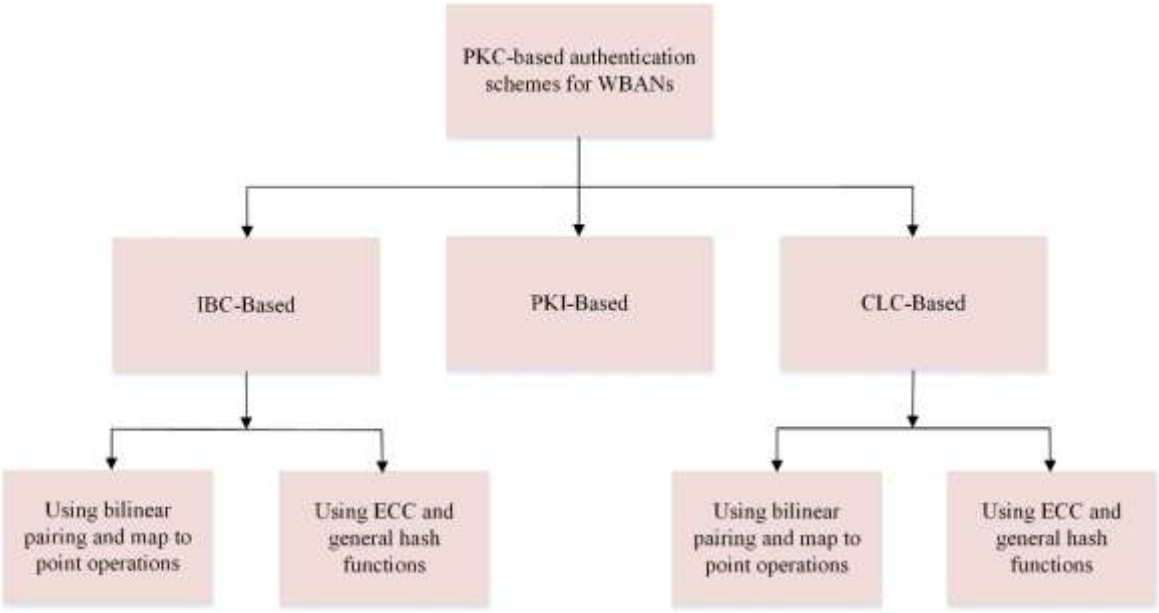

Figure 2.2: Classification of PKC-Based Authentication Schemes for WBANs

Source: Author

2.3.1.1. PKI based Signature Schemes

PKI-based schemes were first introduced and made publicly known by (Diffie, W., 1976). The PKI involve a key pair, the private and public key used during message signing and verification. These keys are non-identical but are mathematically related. In PKI, a trusted authority commonly referred to as a certificate authority (CA) is mandated to issue certificates to entities. To create a certificate, an entity's public key is linked to its identity. The certificate is then signed with a certification authority's (CA) private key. The certificate can be validated using the CA's public key, which allows recipients to trust that the key belongs to the sending entity. Nevertheless, PKI-based schemes involve computationally expensive processes like certificate generation, storage, transmission, verification, and revocation, which are unsuitable for resource-constrained environments like WBANs.

In PKI, a given PD sensor node SN_{PD} makes a registration by submitting its real identity RID_{PD} to a certificate authority (CA). The CA checks the validity of the sensor's RID_{PD} from the records of manufacturer. If the RID_{PD} is valid, the CA creates the public key pk_{PD}, the private key sk_{PD}, and certificate $Cert_{PD}$ for the sensor. The CA then maintains

certificate $Cert_{PD}$ and the respective public key pk_{PD} in a local database. When a sensor node is determined to be malicious, its certificate is invalidated and added to a certificate revocation list (CRL) for future reference.

The certificate $Cert_{PD}$ is signed by the CA using his master secret key sk_{CA} and validated using the public key of CA pk_{CA} . The $Cert_{PD}$ binds the PD's public key pk_{PD} and the real identity RID_{PD} together for traceability. During communication, the PD uses her private key sk_{PD} to generate signature σ_{PD} on message m_{PD}, and sends tuple $\{m_{PD}, \sigma_{PD}, Cert_{PD}\}$ to the application provider. After receiving the message, the AP node checks absence of the certificate $Cert_{PD}$ in the CRL. If it is absent, the AP verifies the $Cert_{PD}$ using the CA's master public key pk_{CA}. If valid, the AP continues to verify signature σ_{PD} on message m_{PD} using the PD's public key pk_{PD}. The AP accepts the message m_{PD} when both $Cert_{PD}$ and σ_{PD} are valid. Otherwise rejects m_{PD}.

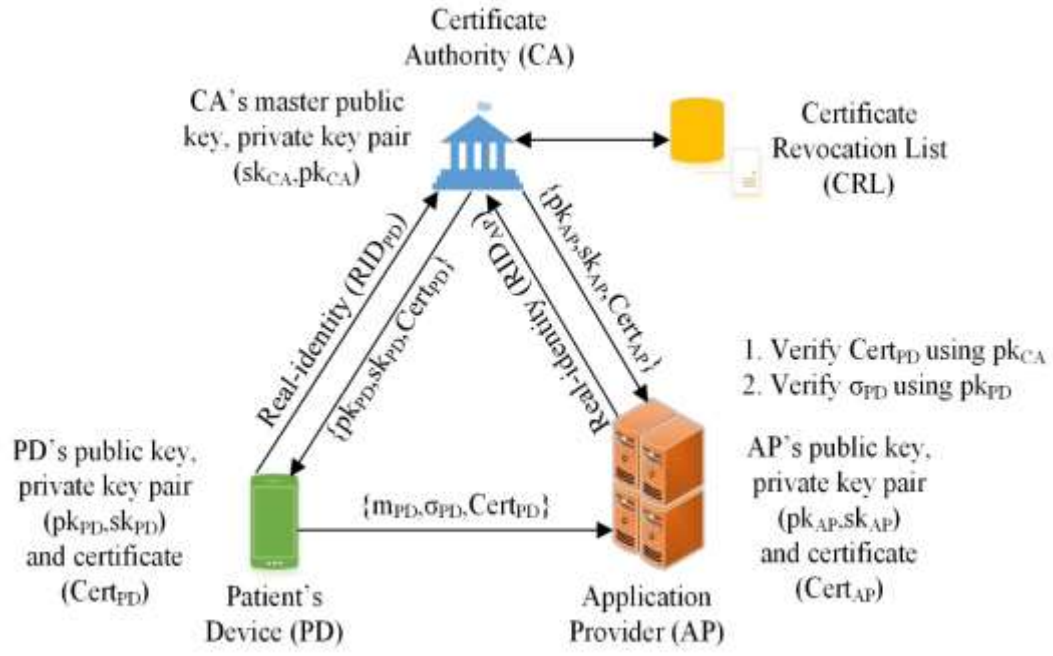

Figure 2.3: Basic PKI Authentication Process

Source: Author

Several PKI- based schemes have been designed by various authors as discussed below:
Xiong Li et al., (2017) designed a protocol that preserves anonymity and allows for key agreement and mutual authentication for wearable sensors in WBANs. The protocol uses XOR operations and hash functions to achieve node confidentiality, mutual authentication, and efficiency. The security of the scheme is rigorously demonstrated through formal proof utilizing BAN logic, along with informal analysis. Nevertheless, the scheme encounters computational overheads as a limitation.

Omala et al., (2018) suggested a novel approach for protecting patient data in WBANs through a heterogeneous signcryption technique with an integrated keyword search that uses signcrypted keywords and designated testers to safeguard patient data. The scheme uses confidentiality and authenticity properties to prove security against keyword-guessing attacks. However, computational overheads affect the efficiency of the scheme.

Koya & P. P, (2018) introduced a method for achieving mutual authentication and establishing secure key agreements in WBANs while maintaining anonymity. The scheme uses physiological signals to counter impersonation attacks on hub and sensor node. BAN logic formally proves the scheme's security against typical WBAN attacks. However, the scheme is computationally infeasible for WBANs.

Kompara et al., (2019) designed a novel authentication and key agreement approach for WBANs that utilizes hash functions and XOR operations to ensure anonymity and untraceability of users. Formal and informal analysis confirms the safety of the scheme. Nevertheless, the scheme has computational overheads that make it unsuitable for WBANs.

Xiong et al., (2022) presented a signcryption scheme for flexible heterogeneous WBAN environment. The security of the scheme is achieved by enabling body sensors to encrypt sensitive data using the PKI's management system public key and then uploading it to a server in the cloud, which conducts an equivalence test on the ciphertext. Despite the security achievements of the above-discussed schemes, they suffer from one common problem, i.e., certificate management complexity, which makes them unsuitable for WBANs.

Table 2.1

A Summary Review of the PKI-Based Authentication Schemes

Scheme	Approach	Strength	Weakness
Xiong. Li et al., 2017	PKI	Achieves confidentiality, mutual authentication and efficiency	Certificate management problem
Omala et al., 2018	Bilinear Pairing, PKI	Keyword search feature, secure against keyword guessing attack.	Certificate management problem, bilinear pairing operation complexities
Koya & P. P., 2018	PKI Physiological signals	Counters sensor and hub node impersonation attack	Certificate management problem
Kompara et al., 2019)	PKI	Provides anonymity and untraceability	Certificate management overheads
Xiong et al., 2022	Bilinear pairing, PKI	Provides confidentiality, unforgeability and keyword search with equality test	Decreased efficiency due to bilinear pairing operations and certificate management problems

2.3.1.2. IBC-Based Signature Schemes

To address the challenges associated with management of public key certificate, Shamir, (1984) introduced the IBC-based scheme. In IBC schemes, users use identification details such as a sensor's serial number or manufacturer details to generate their public keys. The Network Manager (NM) then provides the user with the corresponding private key. This eventually removes the overhead associated with certificate management.

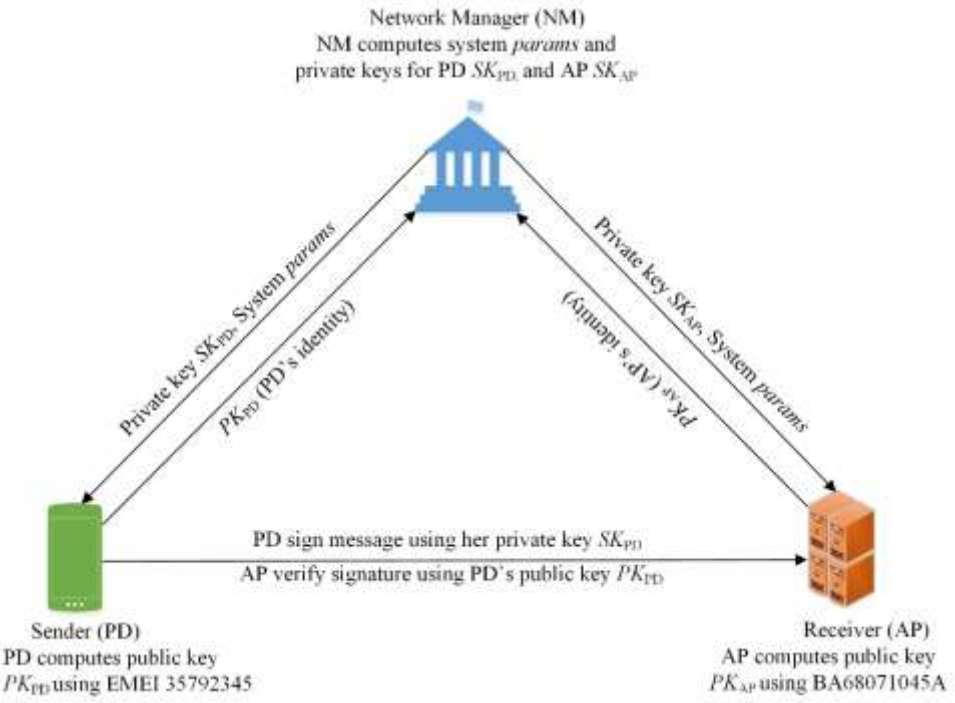

Figure 2.4: Basic Structure of IBC Based Scheme

Source: Author

To illustrate how IBC works, let's assume the sender patient's device (PD) and the receiver application provider (AP) are users in an IBC system. First, PD and AP will submit their identities, which are their public keys, e.g., EMEI35792345 and BA68071045A, to the NM. The NM will verify their identities and generate their corresponding private keys using the NM's master secret key. For PD to send AP a message, PD has to sign the message with its private key, and AP verifies the received signature using PD's public key, which is publicly known. Also, AP can sign and communicate with PD, and PD can use the same process to confirm the signature. In this case, the NM has authority over the private key of all users and can impersonate a user and forge her signature. Therefore, schemes based on IBC suffer from inherent "key escrow" issue. An IBC signature scheme comprises four main algorithms, which are defined below:

Setup: The NM initializes the scheme by inputting a security parameter λ and outputs a NM's secret key sk_{NM}, NM's public key pk_{NM}, and system parameters $params$. The system $params$ and master public key pk_{NM}, are made public while master secret key sk_{NM}, is secretly reserved by the NM.

Key generation: The NM inputs PD's identity (public key pk_{PD}), system $params$, and master secret key sk_{NM}, to this algorithm and generates PD's private key sk_{PD}.
Signature generation: The PD inputs message m_{PD}, , his private key sk_{PD} and some system parameters to this algorithm to generate signature $\sigma_{PD} = sign(m_{PD}, sk_{PD})$.
Signature verification: The AP takes some system parameters, PD's public key pk_{PD}, signature σ_{PD}, and message m_{PD} as inputs. If σ_{PD} is valid, accepts message m_{PD}. Otherwise rejects m_{PD}.

IBC based signatures are further categorized into bilinear pairing and elliptic curve cryptography (ECC). A number of schemes based on bilinear pairing have been designed as reviewed below:

Dai et al., (2018) proposed an energy-efficient scheme for WBANs authentication that uses a bilinear pairing technique to achieve efficiency, security, and privacy. BAN logic-based formal analysis proves the scheme is secure. However, bilinear operations lower the efficiency of their scheme. Deng & Shi., (2018) introduced a streamlined remote authentication scheme aimed at ensuring user traceability and client identity in situations involving medical disputes. The approach utilizes a hash chain of keys as a means to minimize the overheads associated with encryption and decryption. The scheme's security is established through formal analysis in the Random Oracle Model. Nevertheless, pairing operations reduce efficiency.

Jegadeesan et al., (2020) presented another protocol that uses the controller to authenticate users anonymously in WBANs. The scheme enhances performance by incorporating privacy features and a tracking system that enables the disclosure of the true identification of any malicious user. There is, however, reduced efficiency from bilinear operations. Zhang et al (2021) suggested a streamlined and secure scheme for anonymous authentication in WBANs, which attains user anonymity through the utilization of a random value and hash function. Intensive security analyses prove the scheme resilient to common attacks. However, the scheme is susceptible to impersonation attacks. Umar et al., (2021) designed an efficient scheme that anonymously authenticates users using signal propagation characterization. The scheme utilizes distinct variation profiles of received signal strength (RSS) to conceal the nodes' identities, thus achieving anonymity. Security

and performance analysis confirm the scheme is resilient against typical attacks. Nevertheless, the scheme suffers from computational overheads. Despite the advantages, bilinear pairing-based CLC schemes suffer high computation costs, rendering them inefficient for WBANs. Based on elliptic curve cryptography, numerous IBC-based schemes have been proposed as discussed below:

Jahan et al., (2018) proposed a mechanism for end-to-end WBAN authentication that achieves efficacy in the context of communication and computation by utilizing a secret session key. Security analysis which is done both formally and informally proves the scheme resilient against common attacks. Nevertheless, NS-3 simulator evaluates the scheme's influence on various network parameters, and adequate network performance is obtained.

Omala Andrew, (2018) introduced a provably secure signcryption scheme that utilizes an access control protocol to obtain the security and confidentiality of streamed medical data from a network of heterogeneous devices. Formal security analysis conducted in the Random Oracle Model proves the scheme's resistance to Indistinguishability against an Adaptively Chosen Ciphertext Attack and Unforgeability against an Adaptively Chosen Message Attack. Ji et al., (2018) designed an authentication protocol for WBANs that ensures conditional privacy preservation, providing protection against potential malicious actions by a WBAN client. The big data services approach enables secure and efficient processing of physiological data. Improved scheme performance is achieved through batch authentication of multiple WBAN clients. However, the TA could impersonate a client; thus, the scheme is not resilient to impersonation attacks.

Meng, (2019) devised a novel WBAN authentication protocol that incorporates independent sessions to achieve forward secrecy of session keys. Additionally, the scheme employs a combination of hash and XOR operations to enhance its efficiency. Security analysis conducted formally using BAN logic proves the scheme is resilient to common attacks, while verification is done by the AVISPA simulation tool. Xie et al., (2019) designed an efficient authentication protocol using elliptic curve-based signatures and authentication algorithms to achieve secure communication. The efficiency of the scheme is realized through batch authentication, and its security is proved through rigid security

analysis. Wu et al., (2020) suggested a novel protocol for mutually authenticating WBANs that employs a secure session key to ensure session unlinkability and forward/backward confidentiality in WBANs. The protocol leverages XOR operations and one-way hash functions to improve efficiency while maintaining robust security measures.

Shuai et al., (2020) proposed an authentication protocol that is both efficient and privacy-preserving, utilizing elliptic curve cryptography as the underlying cryptographic mechanism. The scheme adopts certificateless identity-based cryptography to achieve security and efficiency in a multi-server architecture. Security analysis which is carried out both formally and informally prove the scheme resistant to possible attacks. Yang et al., (2022) suggested scheme for anonymous authentication of users in cloud-based WBANs that prioritizes security, privacy, and efficiency, employing an elliptic curve authentication protocol. Formal security analysis and verification prove the scheme is resistant to common attacks. Ramadan et al. (2023) presented an identity-based signcryption protocol for telemedicine systems with an equality test feature. The scheme achieves confidentiality and unforgeability in the ROM. Nevertheless, the scheme suffers from the key escrow problem, high computation and communication costs due to bilinear pairing operations, and a lack of sender authentication. The above-discussed IBC-based schemes suffer from one major problem, i.e., the key escrow problem. This makes them insecure for WBANs. Table 2.2 provides a summary of the above-discussed schemes.

Table 2.2

A Summary Review of the IBC-Based Authentication Schemes

Scheme	Approach	Strength	Weakness
Dai et al., 2018	IBC Bilinear pairing	Achieves efficiency, security and privacy	High computational overheads, key escrow problem
Deng & Shi, 2018	IBC Bilinear Pairing	Provides for traceability and user revocation	High computational overheads, key escrow problem
Jegadeesan et al., 2020	IBC based on Bilinear Pairing	Provides Privacy preservation, non-repudiation, unlinkability, security against replay attack, and bogus message attack	Key escrow problem., Reduced efficiency due to bilinear pairing operations.

Zhang et al., 2021	IBC, Bilinear Pairing	Provides user anonymity, security against privileged insider attack other Typical WBAN attacks	Key escrow problem., Reduced efficiency due to bilinear pairing operations
Umar et al., 2021	IBC, Bilinear Pairing	Achieves anonymity, efficiency and security	High computational overheads, key escrow problem
Jahan et al., 2018	IBC based on ECC	Supports mutual authentication, resist user masquerading attack, secret gateway guessing attack and replay attack	Susceptible to key escrow problem
Z. Li & Zhou, 2018	CLC and IBC	Both formal and informal security analysis conducted	Key escrow problem on receiver node
Ji et al., 2018	CPP, ECC based IBC	Supports batch authentication	Susceptible to key escrow problem
Meng, 2019	IBC	Untraceability, session key forward secrecy, minimal hash functions and XOR operations	Susceptible to key escrow problem
Xie et al., 2019	ECC based IBC, CPP	Conditional privacy preservation, batch authentication	Susceptible to key escrow problem
Wu et al., 2020	IBC	Uses only XOR and hash functions. Secure against sensor node capture attack Provides forward/backward security	No formal security analysis done Susceptible to key escrow problem
Shuai et al., 2020	Certificateless IBC, ECC, Multi-tier architecture.	Provides forward secrecy, anonymity, untraceability	Susceptible to key escrow problem
Yang et al., 2022	Cloud based, ECC	Provides perfect forward secrecy, privacy preservation, secure against common attacks	Susceptible to key escrow problem

2.3.1.3. CLC-Based Schemes

To solve the key escrow issue, a CLC mechanism was developed by (Al-Riyami & Paterson, 2003). In CLC-based schemes, the network manager (NM) generates and sends a partial private key to a user, who then creates the full private key. The full private key consists of the partial private key that corresponds to it, and a secret random value provided

by the user. Consequently, the NM doesn't have the knowledge of the user's private key, effectively resolving the issue of key escrow.

Suppose the sender sensor node PD wants to transmit health message to the receiving node AP. First, PD and AP will submit their real identities (RIDs) to the NM and request partial private keys. Upon verifying their identities, the NM will use its master private key to generate two partial private keys, one for PD and the other for AP. The two will then take their respective partial private keys, and each picks a random integer to compute their keys (i.e., the public and private keys). For PD to send AP a message, she has to sign the message with her private key, and AP validates the received signature using PD's public key, which is publicly known. AP can also sign and send a message to PD, and PD can verify the signature using the same method. In this case, NM does not have full control over users' private keys. Therefore, it cannot forge valid signatures; thus, the key escrow problem in CLC is solved.

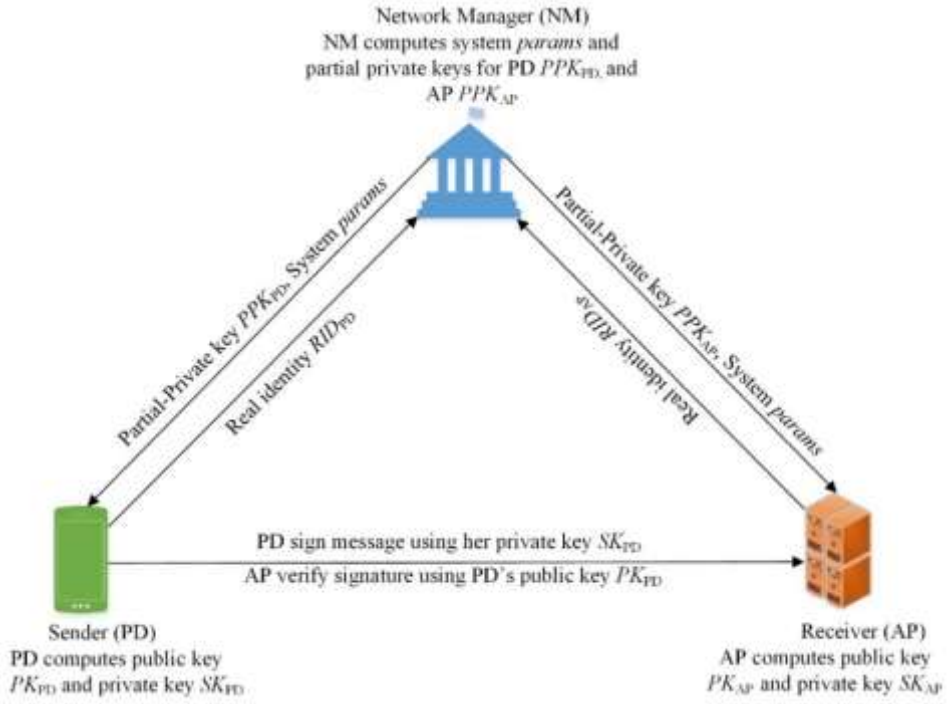

Figure 2.5: Basic Structure of CLC Based Scheme

Source: Author

A CLC signature scheme comprises five main algorithms, which are defined below:

Setup: The NM initializes the scheme by inputting a security parameter λ and outputs a master secret key sk_{NM}, a master public key pk_{NM}, and system parameters $params$. The system $params$ and master public key pk_{NM}, are made public while master secret key sk_{NM}, is concealed by the NM.

Partial private key generation: The NM inputs PD's real identity RID_{PD}, system $params$, and master secret key sk_{NM}, to this algorithm and generates user's partial private key ppk_{PD}.

Key generation: The user inputs the partial private key ppk_{PD}, a secretly chosen random integer, and the system parameters $params$ to this algorithm and generates his private-public keys pair.

Signature generation: The sender inputs message m_{PD}, his private key sk_{SN} and some system parameters $params$ to this algorithm to generate signature $\sigma_{PD} = sign(m_{PD}, sk_{PD})$.

Signature verification: The receiver takes some system parameters *params*, sender's public key pk_{PD}, signature σ_{PD}, and message m_{PD} as inputs. If σ_{PD}, is valid, accepts message m_{PD}. Otherwise rejects m_{PD}.

Like IBC based schemes, CLC schemes are also classified into bilinear pairing and ECC. Several authors have proposed bilinear pairing based CLC schemes as discussed below:

Fagen. Li, (2018) designed a scheme to anonymously control access in WBANs to achieve cost effectiveness using a novel signcryption protocol. The scheme undergoes formal analysis to prove its security against typical attacks. Nevertheless, it suffers from complex computations unsuitable for WBANs. Shen et al., (2018) presented a lightweight certificateless authentication protocol that enhances WBAN capabilities using cloud services. The scheme further adopts anonymity to safeguard the privacy of users. However, the protocol suffers from a lack of forward secrecy and reduced efficiency due to unnecessary hash operations. Abiramy et al., (2018) designed a secure certificateless signcryption algorithm for WBAN that uses the homomorphic property to achieve secure computation. Experimental results prove that the scheme is efficient. Konan & Wang, (2019) developed a secure authentication scheme that combines bilinear pairing and ECC operations to achieve security. Subscriber authentication and provider validation guarantee

security against impersonation, while batch authentication improves efficiency. Based on the ECC cryptosystem, numerous authors have designed and presented CLC-based protocols as discussed below:

Zhou (2019a) proposed a protocol for mobile health systems based on certificateless signcryption as an improvement to Zhang et al.'s scheme. The author applied elliptic curve cryptography to achieve confidentiality and unforgeability, as well as improving a little on computation and communication costs in comparison to the original scheme. However, their scheme is relatively expensive computationally and lacks a conditional anonymity security feature, thus exposing the device's real identity to the public. Liu et al. (2020) designed a streamlined data access control scheme by leveraging the signcryption technique for improved efficiency. A pairing-free RSA cryptosystem is applied to make the scheme more applicable in the industry in terms of efficiency. Formal analysis proves the scheme resilient to typical security attacks. The scheme, however, lacks anonymity. Fotouhi et al. (2020) proposed a lightweight authentication protocol that utilizes two-factor authentication to achieve resilience against common security attacks in WBAN for healthcare IoT. However, the scheme is less efficient due to double authentication. Xu et al. (2020) designed a secure method for mutual authentication in WBANs based on blockchain technology, wherein the patient's biometric data is utilized for authenticating the sensor nodes. Formal and informal analysis proves the scheme's safety while a comparative analysis attests to its efficiency. The scheme, however, incurs storage overheads.

Rehman et al. (2021) developed a hybrid authentication protocol for WBAN that combines physiological signals and lightweight cryptographic methods to mitigate typical security concerns. The scheme's efficiency and security are demonstrated through formal proof of mutual authentication using BAN logic, and also informal verification utilizing AVISPA tools. Noor et al. (2021) introduced a novel framework named "secure channel-free certificateless signcryption scheme" that relies on a hyperelliptic curve to achieve efficiency and security for resource-constrained WBAN devices. In addition to safety, the proposed scheme eliminates the necessity of a safe channel during partial private key distribution. Ullah et al. (2021) designed a signcryption scheme for the internet of health

things based on hyper-elliptic curve certificateless cryptography to achieve anonymity and forward secrecy at the same time. The scheme further proves to achieve confidentiality and unforgeability through formal security analysis in the ROM. Nonetheless, the scheme lacks sender authentication and is a little more expensive computationally.

Almuhaideb (2022) suggested a streamlined and secure authentication scheme for the Intra-BAN Tier, which uses two protocols for emergency and periodic medical reports. The scheme's security is established through formal and informal analysis methods, showcasing improved computational performance. Mandal (2022) presented a provably secure health care system to achieve confidentiality and privacy of data using a certificateless authenticated key agreement protocol. The scheme is computationally efficient, and formal security analysis proves the scheme's ability to offer session key security in addition to other security requirements. Zhang et al. (2024) proposed a certificateless signcryption scheme for internet of medical things (IoMT) safe data communication based on zero knowledge proof. Their scheme achieves confidentiality and unforgeability, as well as improved communication efficiency in comparison to other relevant schemes. However, Zhang et al.'s scheme lacks a sender authentication security feature and is expensive in terms of communication and computation.

The above ECC-based schemes have varying drawbacks. Nevertheless, most of them suffer computational and communication overheads that reduce efficiency, making them unsuitable for WBAN environments. Table 2.3 summarizes the above CLC discussed schemes.

Table 2.3

A Summary Review of the CLC-Based Authentication Schemes

Scheme	Approach	Strength	Weakness
F. Li, 2018	CLC, Bilinear Pairing	Achieves anonymity, authentication confidentiality, non-repudiation and integrity	High Computational overheads from bilinear pairing
Shen et al., 2018	CLC, ECC Based, cloud aided	Achieves anonymity, reduced energy consumption, secure session key and operational efficiency.	Lack of forward secrecy, high computations from unnecessary hash functions
Abiramy et al., 2018	CLC, uses homomorphic property based on bilinear cryptosystem	Reduces energy consumption and solved key escrow problem	Bilinear operations increase computational costs
Konan & Wang, 2019	CLC, combination of ECC and Bilinear pairing.	Provides for subscriber authentication, provider validation, session key generation and anonymity for clients. Solves impersonation	High computational cost due to bilinear pairing operations
Liu et al., 2020	CLC, RSA based ECC	Provides authentication, confidentiality, integrity, public ciphertext verification, and non-repudiation	Lacks anonymous user identification
Jegadeesan et al., 2020	CLC, Bilinear Pairing	Provides for data integrity, conditional privacy preservation, anonymity, and other common WBAN attacks	High computational cost due to bilinear pairing operations

Fotouhi et al., 2020	CLC, Two factor authentication.	Achieves perfect forward security, untraceability and resilience against the common types of attacks.	Two factor authentication increases computational cost
Xu et al., 2020	CLC, Block-chain based	Incorporates biometrics and conducts both formal and informal security analysis	Increased storage cost
Rehman et al., 2021	CLC, hybrid ECG and lightweight cryptography	Solves key escrow problem using dynamic key update, base station compromise and provides for untraceability	Reduced efficiency due to bio-key extraction procedure
Noor et al., 2021)	CLC, hyperelliptic curve cryptography	Achieves confidentiality, anonymity, resistance against unauthorized users, integrity	High computational cost
Almuhaideb, 2022	CLC, ECC based	Provides for emergency and periodic authentication, security against replay and MITM attack, session key disclosure attack, impersonation attack	Double authentication protocols decrease efficiency
Mandal, 2022	CLC, ECC based	Solves Key Escrow problem, provides confidentiality and anonymity of users.	High computational cost

2.3.2. Techniques for Designing a Signcryption Protocol

To address the security and efficiency issues in WBANs, researchers have proposed a number of techniques for designing a secure and efficient signcryption protocol to achieve security of the message and participant in the WBAN communication network. For instance, Omala et al. (2018) suggested a public key infrastructure (PKI) novel approach for protecting patient data in WBANs through a heterogeneous signcryption technique with an integrated keyword search that uses signcrypted keywords and designated testers to safeguard patient data. Koya & P. (2018) proposed a PKI-based authentication scheme that used the physiological signals to counter impersonation attacks on the hub and sensor node.

Another protocol was suggested by Kompara et al. (2019). The scheme is PKI in nature and utilizes hash functions and XOR operations to ensure anonymity and untraceability of users. Using the same approach, Xiong et al.(2022) presented a signcryption scheme for flexible heterogeneous WBAN environments. The security of the scheme is achieved by enabling body sensors to encrypt sensitive data using the PKI's management system public key and then uploading it to a server in the cloud, which conducts an equivalence test on the ciphertext. All the aforementioned schemes adopted the PKI approach in their design. This approach, however, is resource-intensive.

To improve efficiency, certificateless identity-based schemes were introduced. Dai et al. (2018) proposed an energy-efficient scheme for WBANs authentication that uses a bilinear pairing technique to achieve efficiency, security, and privacy. Deng & Shi. (2018) introduced another streamlined remote authentication scheme aimed at ensuring user traceability and client identity in situations involving medical disputes. The approach utilizes a hash chain of keys as a means to minimize the overheads associated with encryption and decryption. Zhang et al. (2021) suggested a streamlined and secure scheme for anonymous authentication in WBANs, which attains user anonymity through the utilization of a random value and hash function. Umar et al. (2021) designed an efficient scheme that anonymously authenticates users using signal propagation characterization. The scheme utilizes distinct variation profiles of received signal strength (RSS) to conceal the nodes' identities, thus achieving anonymity. All the above techniques used a bilinear pairing approach, which, despite being secure, incurs computational complexities.

To minimize computational inefficiencies, more schemes that adopted a pairing-free approach were suggested. Jahan et al. (2018) proposed a mechanism for end-to-end WBAN authentication that achieves efficacy in the context of communication and computation by utilizing a secret session key. Omala Andrew (2018) introduced a provably secure signcryption scheme that utilizes an access control protocol to obtain the security and confidentiality of streamed medical data from a network of heterogeneous devices. Meng (2019) devised a novel WBAN authentication protocol that incorporates independent sessions to achieve forward secrecy of session keys. Additionally, the scheme employs a combination of hash and XOR operations to enhance its efficiency. Xie et al. (2019)

designed an efficient authentication protocol using elliptic curve-based signatures and authentication algorithms to achieve secure communication. Wu et al. (2020) suggested a novel protocol for mutually authenticating WBANs that employs a secure session key to ensure session unlinkability and forward/backward confidentiality in WBANs. The protocol leverages XOR operations and one-way hash functions to improve efficiency. Shuai et al. (2020) proposed an authentication protocol that is both efficient and privacy-preserving, utilizing elliptic curve cryptography as the underlying cryptographic mechanism. The scheme adopts certificateless identity-based cryptography to achieve security and efficiency in a multi-server architecture. Yang et al. (2022) suggested a scheme for anonymous authentication of users in cloud-based WBANs that prioritizes security, privacy, and efficiency, employing an elliptic curve authentication protocol. Although the schemes aforementioned do not involve certificate management, the fact that they are identity-based in nature renders them susceptible to the key-escrow problem.

To address the key-escrow problem, researchers introduced new schemes based on the certificateless cryptography (CLC) technique. Abiramy et al. (2018) designed a secure certificateless signcryption algorithm for WBAN that uses the homomorphic property to achieve secure computation. Konan & Wang (2019) developed a secure authentication scheme by combining bilinear pairing and ECC operations to achieve security. Zhou (2019a) proposed a protocol for mobile health systems based on certificateless signcryption as an improvement to Zhang et al.'s scheme. The author applied elliptic curve cryptography to achieve confidentiality and unforgeability, as well as improving a little on computation and communication costs compared to the original scheme. Liu et al. (2020) designed a streamlined data access control scheme by leveraging the signcryption technique for improved efficiency. The authors applied a pairing-free RSA cryptosystem to make the scheme more applicable in the industry in terms of efficiency. Fotouhi et al. (2020) proposed a lightweight authentication protocol that utilizes two-factor authentication to achieve resilience against common security attacks in WBAN for healthcare IoT. Xu et al. (2020) presented a secure method for mutual authentication in WBANs based on blockchain technology, wherein the patient's biometric data is utilized for authenticating the sensor nodes. Noor et al. (2021) introduced a novel framework named "secure channel-free certificateless signcryption scheme" that relies on a hyperelliptic curve to achieve

efficiency and security for resource-constrained WBAN devices. Ullah et al. (2021) designed a signcryption scheme for the internet of health things based on hyper-elliptic curve certificateless cryptography to achieve anonymity and forward secrecy at the same time. Mandal (2022) presented a provably secure health care system to achieve confidentiality and privacy of data using a certificateless authenticated key agreement protocol. Zhang et al. (2024) proposed a certificateless signcryption scheme for internet of medical things (IoMT) safe data communication based on zero knowledge proof.

2.3.3. Performance Evaluation Techniques

To evaluate the performance of the various schemes deigned by authors in terms of security and efficiency, several techniques have been suggested, some of which have been adopted by various researchers. Below is a discussion of the key techniques applied in the evaluation of performance in WBAN communication. The first method is the formal security proof. Formal security proof utilizes mathematical models under well-defined assumptions to verify the security of a protocol (Ullah, Zeadally, et al., 2021). One of the most commonly used models is the Random Oracle Model. It is particularly useful for certifying WABN protocols, especially in medical systems, which require a lot of security and trust. The model assesses whether protocols meet theoretical standards against the various types of attackers. The next technique is the simulation-based validation. This technique uses special tools to test security protocols against simulated attack scenarios. The commonly used tools include Automated Validation of Internet Security Protocols and Applications (AVISPA) and Scyther (Xu et al., 2020). By conducting attack simulations, an insight into practical resilience is obtained through the assessment of how protocols perform under various attack scenarios. Simulation-based validation is beneficial for identifying certain vulnerabilities, though they may fail to fully capture every real-world condition and are resource constrained. Another technique is the cryptographic validation. This validation technique evaluates specific cryptographic elements of WBAN protocols, such as digital signatures, key management, and encryption techniques, against attacks aimed at confidentiality, integrity, and authenticity. The technique verifies the strength of individual components but may overlook the broader security concerns such as unauthorized access, leading to real-world vulnerability for WBAN systems (Kumar & Hussain, 2023). Other methods used to evaluate performance include energy and latency testing, privacy analysis,

and simulations. The energy and latency testing focus on balancing security with operational efficiency by analyzing the computational load of cryptographic operations and the communication latency introduced by authentication processes (Hasan et al., 2020). Through energy and latency testing techniques, researchers are able to determine cryptographic methods that minimize power consumption and delay, thus prolonging the lifespan of a device. For privacy analysis, user anonymity and data confidentiality are maintained. Protection against data leaks is done using techniques like zero-knowledge proofs and biometric-based authentication. Privacy analysis is necessary for healthcare WBANs, which demand high confidentiality of data (Vyas & Pal, 2020). To evaluate the performance of a protocol in terms of computation cost, a simulation tool like the MIRACL CC library is used to simulate the various cryptographic operations running times, which are used to test the efficiency of the given protocol. On the other hand, network performance can be evaluated using various network simulators, such as the GNS3 simulator, the NS-3 simulator, or the OMNeT++, among others (Kim et al., 2020). These tools help researchers gain some insight regarding the network performance in terms of message throughput, end-to-end delay, and the packet loss ratio.

Several authors have utilized the aforementioned techniques in performance evaluation of their protocols. Xiong Li et al. (2017) validated the security of their scheme through formal proof utilizing BAN logic, along with informal analysis. Deng & Shi (2018) established the security of their scheme formally using the random oracle model. Jahan et al. (2018) used both formal and informal security proof as well as NS-3 simulator to evaluate the scheme's influence on various network parameters. The scheme in Omala Andrew (2018) uses the random oracle model as the formal security proof mechanism. In Meng, (2019), the security analysis is conducted formally using BAN logic to prove the scheme is resilient to common attacks, while verification is done by the AVISPA simulation tool. Ramadan et al. (2023) presented a scheme that uses the random oracle model to verify its security. Similarly, the scheme in Ullah et al. (2021) utilized the random oracle model to validate the security of their scheme. Validations based on formal security proofs are most preferable, as they offer mathematical rigor and structured validation, providing strong evidence that a protocol can withstand specified attack models. This level of assurance is essential in sensitive applications like WBANs, where data confidentiality and patient safety are

paramount. By defining precise adversary models, formal proofs allow researchers to systematically analyze protocol resilience, making it a trusted standard for evaluating security against both theoretical and practical threats. This study therefore adopted both formal and informal analysis and simulation-based validation methods to conduct the performance evaluation of the proposed scheme.

CHAPTER THREE
RESEARCH METHODOLOGY

3.1. Introduction

This section is structured as follows: Section 3.2 presents the study site, and Section 3.3 deals with research design. The method for data collection in the proposed study's scheme is presented in Section 3.4. Data analysis is presented in Section 3.5. Finally, the ethical considerations of the study are given in Section 3.6.

3.2. Study Site

The study was conducted on a PC running in a Linux operating system environment to run simulations at Tharaka University. Linux provides robustness, flexibility, and an extensive toolset for conducting NS-3 simulations. Additionally, Linux offers a reliable and efficient environment for running network simulations by allowing one to delve into various networking scenarios, explore protocol behavior, and easily analyze performance metrics. Therefore, Linux was the ideal platform for conducting NS-3 simulations. The proposed protocol was designed using the elliptic curve cryptography (ECC) technique. The choice of ECC was driven by the desirable features of ECC, which include strong security with a shorter key length compared to traditional public key cryptosystems like RSA and DSA. For instance, a 256-bit ECC key provides similar security to a 3,072-bit RSA key. Therefore, this reduces computational complexity, which eventually makes the ECC approach more efficient. Other ECC desirable features include reduced computational overhead, lower power consumption, efficient use of bandwidth, scalability, and resilience to brute force attacks due to the hardness of ECDLP.

3.3. Research Design

The study adopted both quantitative and qualitative research approaches. For the quantitative approach, the study set up simulation using the NS-3 simulator to simulate the network performance of the proposed schemes and that of other related schemes. The network performance metrics considered include throughput, end-to-end delay, and the packet loss ratio. To generate the running times for the various cryptographic operations considered in this study, the MIRACL CC library was used. The study considered the running times for ECC and bilinear pairing-based point addition, ECC and bilinear pairing-

based scalar multiplication, hash operation, modular inverse operation, bilinear pairing operation, and exponentiation operation. For a qualitative approach, the study adopted theoretical methods to analyze the performance of the proposed scheme and other related schemes, where the data collected was used to compare the performance of the study's proposed scheme with the state-of-the-art schemes. The performance metrics considered were computational cost, communication cost, and the network. The study further adopted theoretical models to prove security of the study's scheme formally, using the Random Oracle Model (ROM), to prove IND-CCA and EUF-CMA. The obtained results were then used to compare the scheme with other existing schemes to ascertain the suitability of the study's scheme in the WBAN environment.

3.3.1. System Model

The study's system model comprises four participants, namely, biosensors, the patient's device (PD), the application provider (AP), and the network manager (NM). The NM and AP form the upper layer of the network, while sensors and PD form the lower layer. The roles of the participants are discussed below:

The Biosensors detect and measure physiological information. This information is sent to an intermediate node such as PDA or hand-held mobile phone. The PD collects and aggregates data from multiple biosensors or wearable devices within the WBAN, acting as a central hub or gateway that collects, processes, and transmits data from various sensors or wearables to a remote receiver or a healthcare system for further analysis or action. The AP collects data from PDs and provides services such as diagnosis and emergency services to the client when needed. It could be a medical system set up in a hospital or a doctor's office. Finally, the NM assumes the responsibility for the overall network management and partial private key generation. The NM is also mandated to register entities and trace their real identities, when necessary, as well as revocation in case of misbehavior.

The study assumed that communication between NM and other entities is secure and reliable, while transmission between PD and AP is insecure and can be compromised. Biosensors are considered trusted entities but have no computing power. PD and AP are untrusted and can easily be compromised. Their computing resources are also limited. The NM has sufficient computing and storage resources and is independent, so it cannot

conspire to perform malicious activity. Finally, all entities are assumed to have a synchronized clock.

3.3.2. Framework of the Proposed Signcryption Scheme

The study's scheme comprises four major algorithms namely; Setup, Registration and Key Generation, Message Signcryption, and Message Unsigncryption.

$Setup$: This is an initialization algorithm executed by NM. It requires an input security parameter λ to output s_{NM} as its master private key and publishes system parameters $params$.

$Registration\ and\ Key\ Generation$: The NM runs this algorithm to register PD and AP. For PD registration, the algorithm requires system $params$ and PD's real identity RID_{PD} as input and outputs PD's pseudo-identity PID_{PD} and partial private key PPK_{PD}. The PD then inputs PPK_{PD} to generate its private-public key pair (SK_{PD}, PK_{PD}). On the other hand, the AP registration requires system $params$ and AP's real identity RID_{AP} as input and outputs AP's partial private key PPK_{AP}. The AP then inputs PPK_{AP} to generate its private-public key pair (SK_{AP}, PK_{AP}).

$Message\ Signcryption$: This algorithm is executed by PD and AP. To perform PD signcryption, the system requires message m_{PD}, system $params$, pseudo identity $PID_{PD,}$ private key SK_{PD} and AP's public key PK_{AP}, as input and the PD outputs a signcrypted message ϱ. To carry out AP Signcryption, the message m_{AP}, system $params$, AP's private key SK_{AP} and PD's public key PK_{PD}, are taken as the input and the AP outputs a signcrypted message ϱ.

$Message\ Unsigncryption$: This algorithm is implemented by the receiving entity. It takes system $params$, its private key SK, the senders public key PK and ϱ as input and produces message m as output if ϱ is valid, otherwise rejects m.

Figure 3.1 provides a framework summary of the above-proposed signcryption protocol

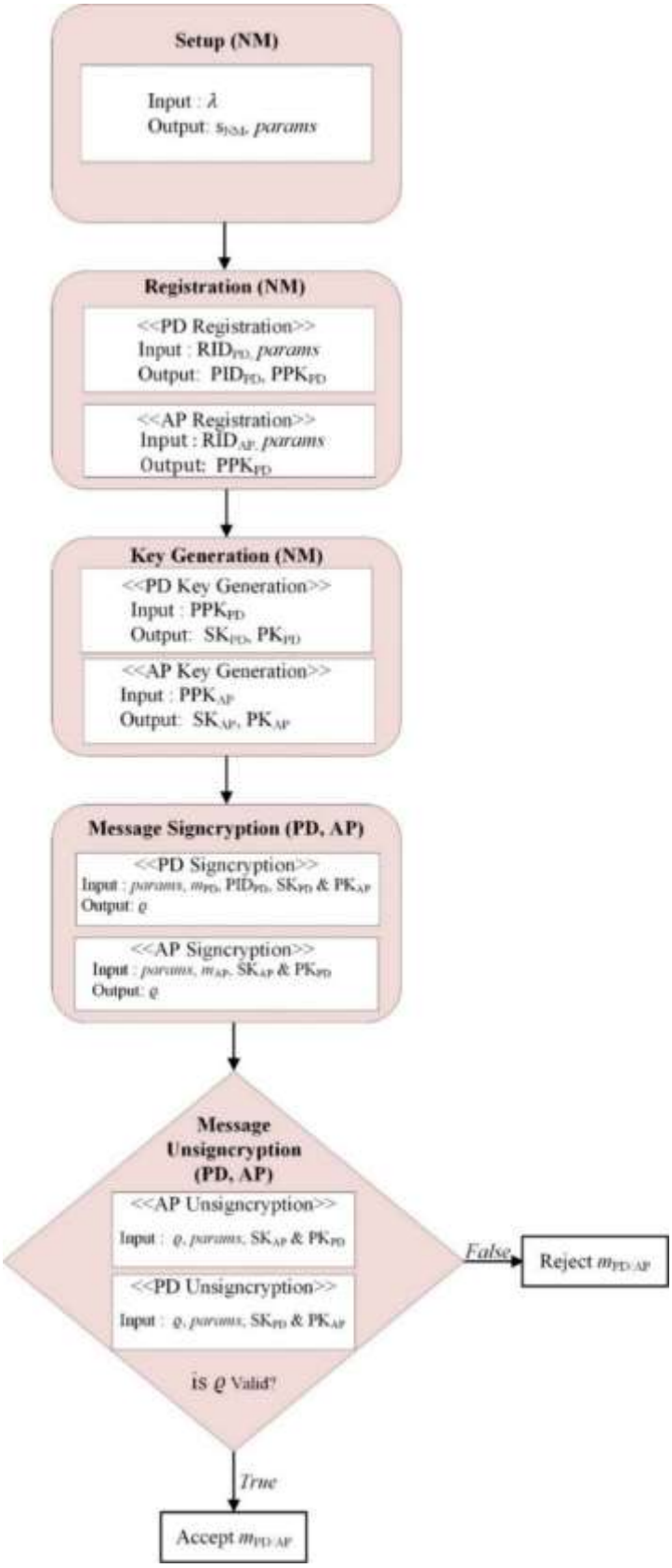

Figure 3.1: Framework of the Proposed Signcryption Protocol

3.4. Data Collection

The study used experiments (simulation) to generate primary data regarding the running times for cryptographic operations in the proposed scheme. A sample of a data set from a simulation experiment is presented in Table 3.1. Further, the study utilized the existing literature to obtain secondary data on the computation and communication costs of other related schemes.

Table 3.1

Notation and Time for Execution of Cryptographic Operations

Source: (Yao et al., 2021)

Notation	Description	Execution Time (ms)
T_{sm_bp}	Bilinear pairing group based scalar multiplication	0.694
T_{sm_ecc}	ECC group based scalar point multiplication	0.3218
$T_{sm\_bp\_s}$	Bilinear pairing group based small scalar multiplication	0.0736
$T_{sm\_ecc\_s}$	ECC group based small scalar multiplication	0.0246
T_{pa_bp}	Bilinear pairing group-based point addition	0.0018
T_{pa_ecc}	ECC based point addition	0.0024
T_{bp}	Bilinear pairing operation	5.086
T_{h}	Operation involving general one-way hash function	0.001
T_{mtp}	Mapping a string to a point in group hash function	0.0992

3.4.1. Experimental Setup

Two sets of simulation experiments were conducted. The first experiment involved the use of the Mult-precision Integer and Rational Arithmetic Cryptographic Library for C/C++ (MIRACL CC) toolkit to generate the running times for various cryptographic operations considered in the proposed scheme (as outlined in Section 3.3). Using the running times generated, the total computation cost for the proposed scheme was computed for both signcryption and unsigncryption algorithms. Similarly, the total computation cost for other related schemes was computed using the same procedure. The data obtained from this experiment was used to evaluate the performance of the proposed scheme in terms of computational cost to determine its efficiency. The next experiment involved simulation of the network. The experiment utilized Network Simulator 3 (NS-3) to evaluate the network

performance of the proposed WBAN protocol in terms of throughput, end-to-end delay, and packet loss ratio. The results obtained were used to compare the network performance of the proposed scheme with related schemes. Figure 3.2 provides a conceptual framework, showing the variables used in network simulation and their relationships. From the figure, the number of nodes and simulation time represent the set of independent variables whose variation strongly affects the outcome of the network performance in terms of end-to-end delay, message throughput, and packet loss ratio, thus the dependent variables. In this experimental setup, the processor speed denotes the intervening variables. This variable will affect the outcome of the independent variables by altering the relationship between the independent and dependent variables; hence, it requires to be controlled; otherwise, it may result in misleading results. For instance, a low-speed processor will result in high end-to-end delays due to processing delays.

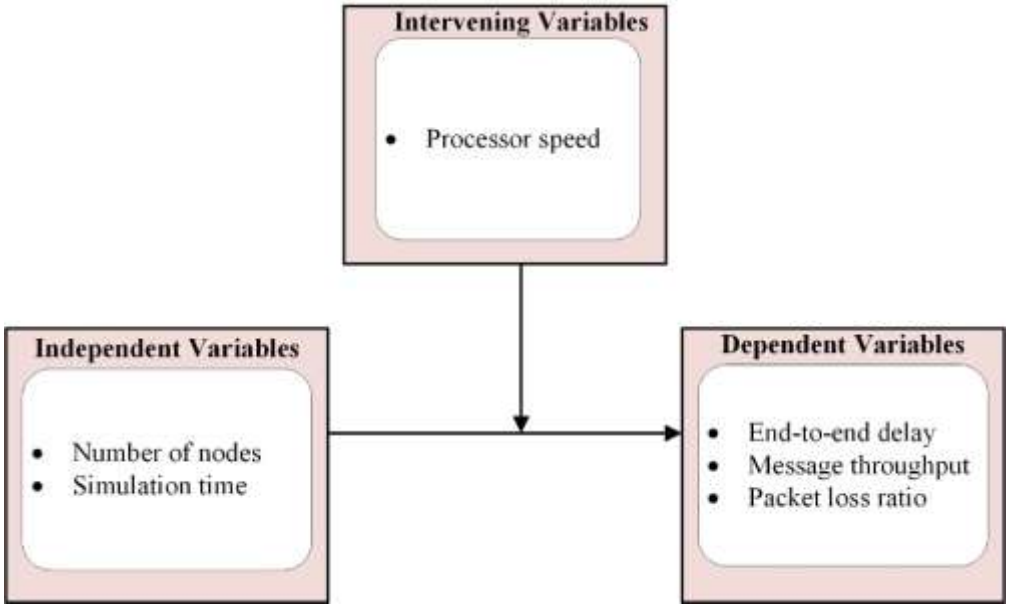

Figure 3.2: Conceptual Framework

Source: Author

3.5. Data Analysis

Subsequent to data collection, primary data was tabulated and analyzed to measure the scheme's performance in terms of computational and communication costs. On the other hand, the secondary data collected from the literature on related work was analyzed, ready

for performance comparison with the proposed scheme in terms of the aforementioned costs. Besides, the study conducted security analysis both formally and informally.

3.5.1. Performance Analysis

Performance analysis was carried out in terms of computational and communication costs. For computational cost, this study evaluated the computational cost of the proposed secure and efficient signcryption protocol in comparison to other related schemes. The research considered the running time as well as the energy cost of the following elliptic curve operations used to construct the proposed scheme: scalar multiplication, point addition, inverse operation, modular exponentiation, and hash operations. The research focused on the number of operations used to perform signcryption and verify the ciphertext through the unsigncryption process. To evaluate the communication cost, the study considered the cost involved in data transmission with regard to the aggregate length of data transmitted within a specified period of time, which has an impact on energy costs. Other aspects of communication considered include message throughput, packet loss ratio, and end-to-end delay. These factors were used to compare the proposed scheme with state-of-the-art schemes.

3.5.2. Security Analysis

The study conducted a security analysis to determine whether the proposed scheme meets the following security requirements: authentication (sender and message), confidentiality, unforgeability, nonrepudiation, key-escrow resistance, availability, forward secrecy, and internal security. The study further analyzed the study's scheme to confirm that it is resilient against common attacks targeting WBANs, including replay attacks, message falsification, impersonation, and MITM attacks. The security model of the proposed scheme considered two adversary types: Type-1 and Type-2. The study defines a Type-1 adversary as an outsider attacker or a regular user who can replace the node's public key with a choice value without accessing the NM's master secret key. On the other hand, the study characterizes a type-2 adversary as an insider attacker, specifically a trusted but curious NM who possesses the master secret key. The NM is expected to be honest and should not replace the node's public key with a choice value.

To conduct a security proof for the proposed scheme, the study considered two games: Game-1 and Game-2. The players of Game-1 are Type-1 adversary Adv_1 and challenger $\mathcal{C}$. The game's rules involve Adv_1 asking some queries and $\mathcal{C}$ answering them correctly. The target of Adv_1 is to compromise the proposed scheme using the answers given by $\mathcal{C}$. If the advantage of Adv_1 in winning Game-1 is negligible, the study argues that the proposed scheme is secure against Adv_1. On the other hand, the players of Game-2 are Type-2 adversary Adv_2 and challenger $\mathcal{C}$. The game's rules involve the Adv_2 asking some queries and $\mathcal{C}$ answering them correctly. The target of Adv_2 is to compromise the proposed scheme using the answers given by $\mathcal{C}$. If the advantage of Adv_2 in winning Game-2 is negligible, the study argues that the proposed scheme is secure against Adv_2.

3.6. Ethical Consideration

This study adhered to the principles regarding research ethics. Firstly, the study obtained an introductory research letter from Tharaka University. Secondly, the research sought approval from the Tharaka University ethics committee. Additionally, this study acquired a research license from the National Commission for Science, Technology and Innovation (NACOSTI). Finally, the researcher upheld integrity by avoiding plagiarism and acknowledging the work done by other researchers through citations and referencing.

CHAPTER FOUR
RESULTS AND DISCUSSION

4.1. Introduction

This chapter provides the results of the study in terms of the proposed scheme construction, security analysis of the proposed study's scheme and a comparison with related schemes, performance evaluation of the scheme and a comparison with other state-of-the-art schemes in terms of computation cost and communication cost, and simulation experiment, as discussed in sections 4.2, 4.3, 4.4, and 4.5, respectively.

4.2. Construction of the Proposed ECC-Based Signcryption Scheme

This section presents the proposed ECC-based secure and efficient certificateless signcryption protocol for a wireless body area network. The protocol entails four major algorithms, i.e., setup, registration and key generation, message signcryption, and message unsigncryption. Table 4.1 provides a description of the notations used in the proposed scheme.

Table 4.1

Notations used in the Proposed Scheme

NOTATION	DESCRIPTION
$\boldsymbol{p}$ **and** $\boldsymbol{q}$	Large prime numbers
$\boldsymbol{G}$	Group of elliptic curve points
$\boldsymbol{E}$	Non-singular elliptic curve
$\{\boldsymbol{s_{NM}}, \boldsymbol{PK_{NM}}\}$	NM's master and public keys
$\{\boldsymbol{H_0}(.),\boldsymbol{H_1}(.),\boldsymbol{H_2}(.),\boldsymbol{H_3}(.)\}$	General One-way hash functions
$\boldsymbol{PD_i}$	Patient's device
$\{\boldsymbol{RID}_{\boldsymbol{PD_i}}, \boldsymbol{PID}_{\boldsymbol{PD_i}}\}$	$PD's$ real identity and pseudo identity
$\{\boldsymbol{\omega_i}, \boldsymbol{\theta_i}\}$	Secret key for PD_i and AP
$\{\boldsymbol{T_i}, \boldsymbol{t_i}\}$	Valid time periods
$\oplus$	XOR operation
$\{\boldsymbol{d_{PD_i}}, \boldsymbol{d_{AP}}\}$	NM's secret key for PD_i and AP PPK generation
$\{\boldsymbol{PPK_{PD_i}}, \boldsymbol{PPK_{AP}}\}$	Partial private keys for PD_i and AP
$\{\boldsymbol{x_{PD_i}}, \boldsymbol{x_{AP}}\}$	PD_i and AP secret key for private key generation
$\boldsymbol{r_{PD_i}}$	PD_i's secret key for message signcryption
$\{\boldsymbol{SK_{PD_i}}, \boldsymbol{PK_{PD_i}}\}$	Private and Public key for PD_i
$\{\boldsymbol{SK_{AP}}, \boldsymbol{PK_{AP}}\}$	Private and public key for AP
$\boldsymbol{\varrho}$	Signcryption
$\perp$	Error
$\{\boldsymbol{m_{PD_i}}, \boldsymbol{m_{AP}}\}$	PD_i and AP message

4.2.1. Setup

The Network Manager(NM) solely initializes the system by performing the following. Inputs $\lambda \in Z^+$as security parameter, randomly picks two large prime numbers p and q and non-singular elliptic curve E defined by the equation $y^2 = x^2 + ax + b$, where $a, b \in F_P$ and $4a^3 + 27b^2 \neq 0$. Selects a generator P for group G, where G are elliptic curve points with prime order q. Randomly picks $s_{NM} \in \mathrm{Z}_q^*$ as its master secret key, and computes its public key as $PK_{NM} = s_{NM}P$. Randomly picks four one-way hash functions: $H_0: \{0,1\}^* \rightarrow \mathrm{Z}_q^*$, $H_1: G \times G \times G \rightarrow \mathrm{Z}_q^*$, $H_2: G \rightarrow \mathrm{Z}_q^*$, $H_3: G \times \{0,1\}^* \times G \times G \times G \rightarrow \mathrm{Z}_q^*$. Finally, the NM publicly publishes system parameters $params$ as $\{p, q, G, P, PK_{NM}, H_0, H_1, H_2, H_3\}$

4.2.2. Registration and Key generation

Registering WBAN nodes, i.e., patient's device (PD) and application provider (AP), is mandatory before nodes can start communication. The PD registers itself by submitting its real identity, such as sensor device serial, to the NM for scrutiny, and upon successful validation, the NM generates a corresponding pseudo-identity and partial private key. The PD then utilizes the partial private key to compute its full public and private key pair. Regarding AP registration, the AP submits its real identity to the NM for scrutiny, and upon successful authentication, the NM computes a corresponding partial private key for the AP. The AP then utilizes the partial private key to compute its full public and private key. The details for registering a particular node are as follows. The guide for PD registration is outlined below:

The PD randomly chooses $\omega_i \in \mathrm{Z}_q^*$ and computes $PID_{i1} = \omega_i P$. Picks its real-identity RID_{PD_i} and sends tuple $\{PID_{i1}, RID_{PD_i}\}$ to NM. Upon successfully scrutinizing RID_{PD_i}, the NM computes $PID_{i2} = RID_{PD_i} \oplus H_0(s_{NM} PID_{i1})$ and submits pseudo-identity $PID_i = \{PID_{i1}, PID_{i2}, T_i\}$ to PD. Meanwhile, the NM records tuple $\{PID_i, RID_{PD_i}\}$ in a secure database. After PID_i generation, the NM continues to compute a partial private key for the PD using the steps below:

The NM randomly chooses $d_{PD_i} \in \mathrm{Z}_q^*$ and computes $D_{PD_i} = d_{PD_i}P$. Computes $\beta_{PD_i} = H_1(PID_i, D_{PD_i}, PK_{NM})$, computes $k_{PD_i} = (d_{PD_i} + \beta_{PD_i} . s_{NM}) mod\ q$. The NM sends

PPK_{PD_i}=$\{k_{PD_i}, D_{PD_i}\}$ to PD as a partial private key. Upon receiving PPK_{PD_i}, the PD checks for its authenticity by verifying the equation $k_{PD_i}P = D_{PD_i} + \beta_{PD_i}PK_{NM}$.

Proof of Correctness

$$k_{PD_i}P = (d_{PD_i} + \beta_{PD_i}.s_{NM})P$$
$$= d_{PD_i}P + \beta_{PD_i}.s_{NM}P$$
$$= D_{PD_i} + \beta_{PD_i}PK_{NM}$$

After successful verification of the PPK_{PD_i}, the PD generates its secret and public key pair using steps below.

The PD randomly chooses $x_{PD_i} \in Z_q^*$ and sets its secret key as $SK_{PD_i} = \{x_{PD_i}, k_{PD_i}\}$, computes $X_{PD_i} = x_{PD_i}PK_{NM}$ and $Y_{PD_i} = k_{PD_i}PK_{NM}$. Finally, the PD sets its full public key as $PK_{PD_i} = (X_{PD_i}, Y_{PD_i})$. The steps for PD registration are outlined below:

Firstly, the AP randomly chooses $\theta_i \in Z_q^*$ and computes its public key $PK_{AP} = \theta_i P$. It then sends tuple $\{RID_{AP}, PK_{AP}\}$ to NM, where RID_{AP} is the real identity for AP. Upon successfully scrutinizing RID_{AP}, the NM randomly chooses $d_{AP} \in Z_q^*$ and computes $D_{AP} = d_{AP}P$, computes $\beta_{AP} = H_1(D_{AP}, PK_{AP}, PK_{NM})$. The NM further computes $k_{AP} = (d_{AP} + \beta_{AP}.s_{NM}) mod\ q$ and sends partial private key $PPK_{AP} = \{k_{AP}, D_{AP}\}$ to AP.

Upon receiving PPK_{AP}, the AP checks for its authenticity by verifying the equation $k_{AP}P = D_{AP} + \beta_{AP}PK_{NM}$.

Proof of Correctness

$$k_{AP}P = (d_{AP} + \beta_{AP}.s_{NM})P$$
$$= d_{AP}P + \beta_{AP}.s_{NM}P$$
$$= D_{AP} + \beta_{AP}PK_{NM}$$

After successful verification of the PPK_{PD_i}, the AP generates its secret and public key pair using the steps below.

The AP randomly chooses $x_{AP} \in Z_q^*$ and sets its secret key as $SK_{AP} = (x_{AP}, k_{AP})$. Next, the AP computes $X_{AP} = x_{AP} PK_{NM}$ and $Y_{AP} = k_{AP} PK_{NM}$, and sets its full public key as $PK_{AP} = (X_{AP} + Y_{AP})$.

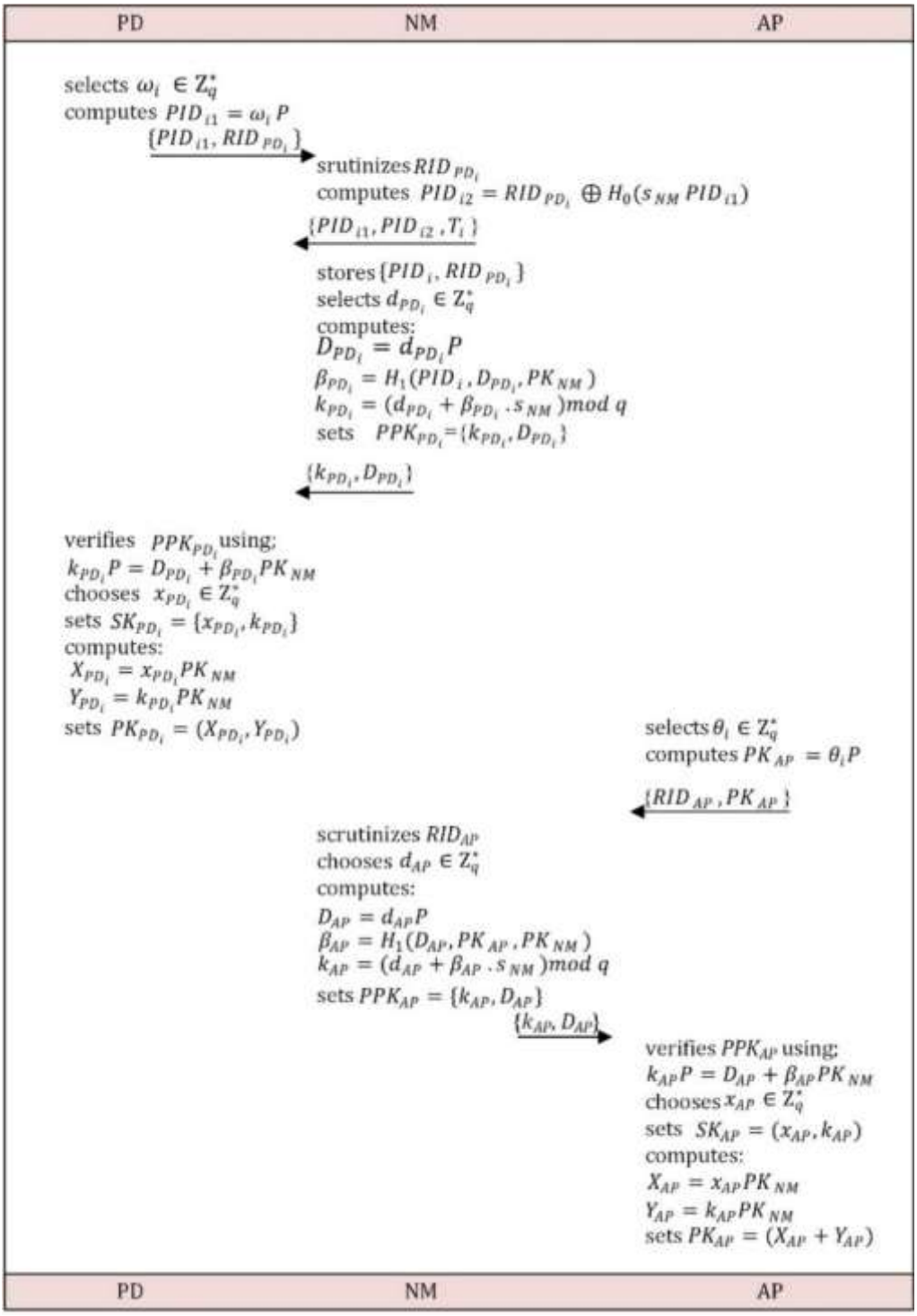

Figure 4.1: Summary of Registration and Key Generation

4.2.3. Message Signcryption

Every health-related message should be signcrypted before transmission to enhance authenticity. The PD to AP Signcryption is carried out as outlined below.

On input of health-related message $m_{PD_i} \in \{0,1\}^*$, system parameters $params$, pseudo identity $PID_{PD_i,}$ private key SK_{PD_i} , and AP's public key PK_{AP}, the PD outputs a signcrypted message ϱ_i. The steps for signcryption are outlined as follows.

Firstly, The PD selects a random value $r_{PD_i} \in Z_q^*$ and computes $R_{PD_i} = r_{PD_i} PK_{AP}$. The PD then computes $b = H_2(R_{PD_i})$ and $c = b \oplus m_{PD_i}$ and $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$. Next, the PD computes $s = {r_{PD_i}}^{-1}(e + SK_{PD_i})$. If $s = 0$, return to step (i). Otherwise, output a signcrypted message $\varrho_i = (c, e, s)$, and send it to AP.

To perform AP to PD Signcryption when the AP needs to send a diagnostic message $m_{AP} \in \{0,1\}^*$ to PD, the AP will use its secret key SK_{AP} and PD's public key PK_{PD_i} to signcrypt message m_{AP} in the same manner that PD to AP signcryption is done.

4.2.4. Message Unsigncryption

Before acting on the signcrypted message, the receiver must run an unsigncryption algorithm to ensure the sender's and message's integrity. The PD to AP Unsigncryption is done using the steps described below.

Upon receiving the signcrypted message $\varrho_i = (c, e, s)$ from PD, the AP extracts pseudo-identity's validity period T_i and timestamp t_i and checks their expiry. If the message is fresh, the AP runs the unsigncryption algorithm by taking system parameters $params$, its private key SK_{AP} and PD's public key PK_{PD_i} as inputs and outputs the original message m_{PD_i}. The steps for unsigncryption are outlined as follows.

Firstly, the AP takes message $\varrho_i = (c, e, s)$ and computes $y = s^{-1}$. It computes $V_{AP} = eyPK_{AP} + yPK_{PD_i}SK_{AP}$, $b' = H_2(V_{AP})$, $m_{PD_i} = b' \oplus c$, and finally $e' =$

$H_3(m_{PD_i}, V_{AP}, PK_{PD_i}, PK_{AP}, PID_{PD_i}, t_i)$. If $e' = e$, AP returns original message m_{PD_i}, otherwise returns error message $\perp$.

For AP to PD Unsigncryption, the PD will perform the unsigncryption process in the same manner that PD to AP unsigncryption is done.

Proof of Correctness

Given $s = {r_{PD_i}}^{-1}\left(e + SK_{PD_i}\right)$, we have $s^{-1} = r_{PD_i}(e + SK_{PD_i})^{-1}$

Therefore, the following correctness holds;

$$V_{AP} = eyPK_{AP} + yPK_{PD_i}SK_{AP}$$

$$= es^{-1}PK_{AP} + s^{-1}PK_{PD_i}SK_{AP}$$

$$= es^{-1}SK_{AP}P + s^{-1}SK_{PD_i}SK_{AP}P$$

$$= \left(e + SK_{PD_i}\right)s^{-1}SK_{AP}P$$

$$= (e + SK_{PD_i})r_{PD_i}(e + SK_{PD_i})^{-1}SK_{AP}P$$

$$= r_{PD_i}SK_{AP}P$$

$$= r_{PD_i}PK_{AP}$$

$$= R_{PD_i}$$

Thus, it is clear that $b' = b$, implying that the receiving device can obtain the original message m_{PD_i} from the sender through the decryption process. Additionally, $e' = e$, which means the receiving device can validate the sender's signature's correctness. Consequently, the proposed signcryption protocol is correct.

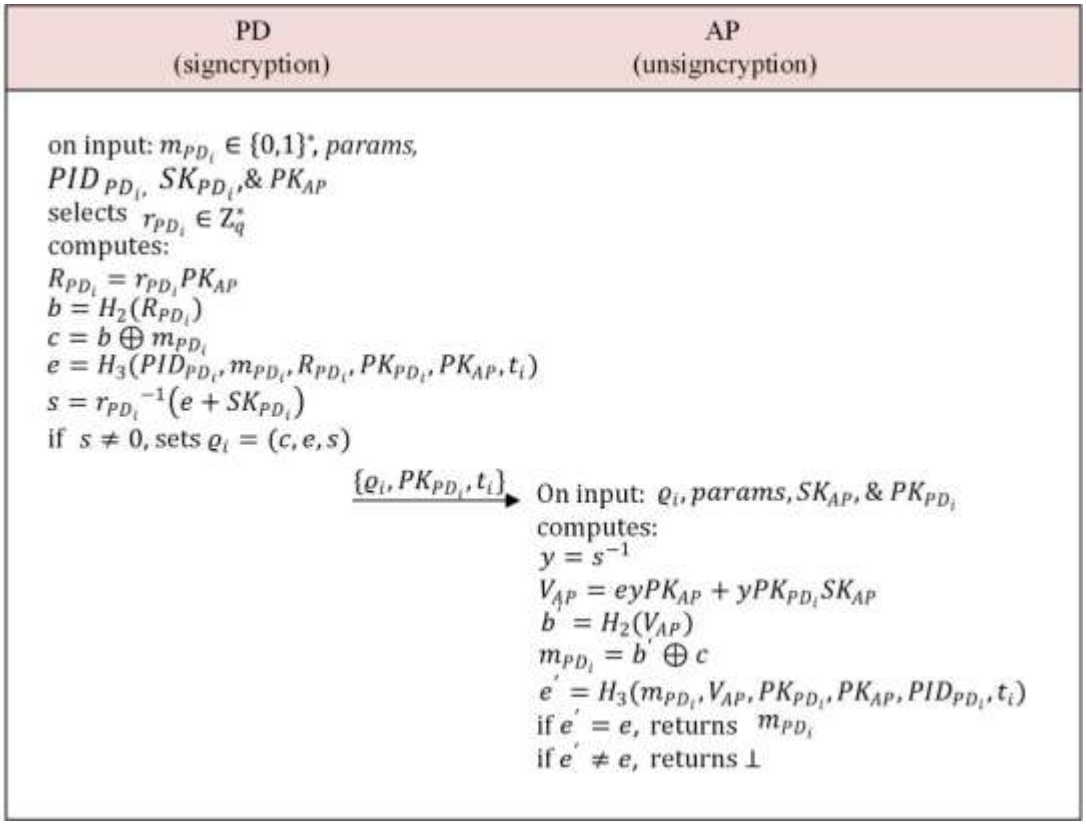

Figure 4.2: Summary of Signcryption and Unsigncryption Algorithms

Source: Author

4.3. Security Analysis

This section conducts a security analysis to prove the security of the proposed study's scheme against possible attacks. The analysis is done both formally and informally

4.3.1. Formal Security Analysis

The formal security scrutiny is conducted to prove confidentiality and unforgeability through formal security proof. The study uses the Random Oracle Model (ROM) to demonstrate the proposed scheme's Indistinguishability under Chosen Ciphertext Attack (IND-CCA) and Existential Unforgeability under Chosen Message Attack (EUF-CMA).

4.3.1.1. Confidentiality

The proposed signcryption scheme combines digital signature and encryption techniques in a single logical step. The encryption property is responsible for the confidentiality, which ensures the patient's data remains private and inaccessible to unauthorized users. The study uses Theorem 1 and 2 to prove confidentiality of proposed scheme.

Theorem 1: Assume that adversary Adv_1 can win Game 1 with a non-negligible advantage $\mathcal{E}' \geq \frac{\varepsilon}{(q_{H_0}+q_{H_1}+q_{H_2}+q_{H_3}+q_{Sig}+q_{Unsig})}$, in ROM after $q_{H_i}(i = 0, \ldots, 3)$ hash queries, q_{Sig} signcryption query and q_{Uns} unsigncryption query. Then, there exists a challenger $\mathcal{C}$ who can solve CDH problem with a minimum advantage $\mathcal{E}'$ as defined at the end of the proof.

Proof: Suppose (P, aP, bP) is an instance of CDH problem, where $a, b \in \mathrm{Z}_q^*$. We show how challenger $\mathcal{C}$ in Game 1 interacts with adversary Adv_1 to compute $C = abP$.

Setup: The challenger $\mathcal{C}$ executes the setup algorithm to generate the system parameters $params$ as $\{p, q, G, P, PK_{NM}, H_0, H_1, H_2, H_3\}$ and a master private key s_{NM}. Note, the challenger $\mathcal{C}$ shares the $params$ with Adv_1 but keeps s_{NM} a secret. To ensure consistency of the queries and responses to ROM, the challenger $\mathcal{C}$ maintains lists $L_{H_i}(i = 0, \ldots, 3)$ for hash queries, and lists L_{PPK}, L_{SK}, L_{PK}, L_{Sig} and L_{Unsig} for partial private key query, secret key query, public key query, signcryption query, and unsigncryption query, respectively. Note all the lists are initially set to empty.

Phase-I

The challenger $\mathcal{C}$ randomly chooses PID_i^* as the target pseudo identity to be challenged. At this point, the study adopts the irreflexivity assumption (A. A. O. Li, 2018), i.e., given two pseudo identities PID_1 and PID_2, if $PID_1 = \mathrm{PID}_i^*$, then $PID_2 \neq \mathrm{PID}_i^*$ and vice versa.

H_0 query: Adversary Adv_1 submits a query on (α_i, T_i) to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple (α_i, T_i, h_0) in the list L_{H_0} and returns h_0 if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $h_0 \in \mathrm{Z}_q^*$ at random and returns h_0 to Adv_1. Then, challenger $\mathcal{C}$ updates L_{H_0} with tuple (α_i, T_i, h_0).

H_1 query: Adversary Adv_1 submits a query on $(PID_i, D_{PD_i}, PK_{NM})$ to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple $(PID_i, D_{PD_i}, PK_{NM}, \beta_{PD_i})$ in the list L_{H_1} and returns β_{PD_i} if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $\beta_{PD_i} \in \mathrm{Z}_q^*$ at random and returns β_{PD_i} to Adv_1. Then, challenger $\mathcal{C}$ updates L_{H_1} with tuple $(PID_i, D_{PD_i}, PK_{NM}, \beta_{PD_i})$.

H_2 query: Adversary Adv_1 submits a query on (R_{PD_i}) to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple (R_{PD_i}, b) in the list L_{H_2} and returns b if the tuple exists.

Otherwise, $\mathcal{C}$ chooses hash value $b \in \mathrm{Z}_q^*$ at random and returns b to Adv_1. Then, challenger $\mathcal{C}$ updates L_{H_2} with tuple(R_{PD_i}, b).

H_3 query: Adversary Adv_1 submits a query on $(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$ to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple $(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i, e)$ in the list L_{H_3} and returns e if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $e \in \mathrm{Z}_q^*$ at random and returns e to Adv_1. Then, challenger $\mathcal{C}$ updates L_{H_3} with tuple $(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i, e)$.

Partial private key query: Adversary Adv_1 submits a query for the partial private key for PID_{PD_i} to the challenger $\mathcal{C}$. If $PID_i = \mathrm{PID}_i^*$, challenger $\mathcal{C}$ terminates the algorithm. Otherwise, if $PID_i \neq \mathrm{PID}_i^*$, challenger $\mathcal{C}$ performs the following: selects $\eta_i, \phi_i \in \mathrm{Z}_q^*$ at random and computes $D_{PD_i} = \eta_i P - \phi_i P$. Next, challenger $\mathcal{C}$ sets $k_{PD_i} = \eta_i$, $H_1(PID_i, D_{PD_i}, PK_{NM}) = \beta_{PD_i} = \phi_i$ and PPK_{PD_i}=(k_{PD_i}, D_{PD_i}). Finally, Challenger $\mathcal{C}$ returns PPK_{PD_i} to adversary Adv_1 as partial private key and updates list L_{PPK} with the tuple $(PID_i, D_{PD_i}, \beta_{PD_i}, k_{PD_i})$.

Public key query: Adversary Adv_1 submits a public key query for PID_i to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for PID_i query in the list L_{PK} and returns PK_{PD_i} if the query exists. Otherwise, $\mathcal{C}$ recovers tuple $(PID_i, D_{PD_i}, \beta_{PD_i}, k_{PD_i})$ from L_{PPK}. Next, $\mathcal{C}$ chooses $x_{PD_i} \in \mathrm{Z}_q^*$ at random and computes $X_{PD_i} = x_{PD_i} PK_{NM}$ and $Y_{PD_i} = k_{PD_i} PK_{NM}$. Finally, $\mathcal{C}$ returns $PK_{PD_i} = (X_{PD_i} + Y_{PD_i})$ to Adv_1 as public key and updates list L_{PK} with the tuple $(PID_i, k_{PD_i}, x_{PD_i}, PK_{PD_i})$.

Private key query: Adversary Adv_1 submits a query for the private for PID_i to the challenger $\mathcal{C}$. If $PID_i = \mathrm{PID}_i^*$, $\mathcal{C}$ terminates the algorithm. Otherwise, if $PID_i \neq \mathrm{PID}_i^*$, challenger $\mathcal{C}$ performs the following: searches for PID_i query in the list L_{PK} and returns SK_{PD_i} to Adv_1 if the query exists. Otherwise, $\mathcal{C}$ runs partial private key and public key queries to output tuple $(PID_i, k_{PD_i}, x_{PD_i}, X_{PD_i}, Y_{PD_i})$. Finally, $\mathcal{C}$ returns $SK_{PD_i} = (k_{PD_i}, x_{PD_i})$ to Adv_1 as the private key.

Public key replace query: Adversary Adv_1 submits a query for replace the public with an input (PID_i, PK'_{PD_i}) to the challenger $\mathcal{C}$, where $PK'_{PD_i} = X'_{PD_i} + Y'_{PD_i}$, $X'_{PD_i} = x'_{PD_i} PK_{NM}$ and $Y'_{PD_i} = k'_{PD_i} PK_{NM}$. Next, $\mathcal{C}$ sets $X_{PD_i} = X'_{PD_i}$, $Y_{PD_i} = Y'_{PD_i}$,

$k_{PD_i} = k'_{PD_i}$ and $x_{PD_i} = x'_{PD_i}$. Finally, $\mathcal{C}$ updates list L_{PK} with the tuple $\left(PID_i, k'_{PD_i}, x'_{PD_i}, PK'_{PD_i}\right)$.

Signcryption query: Adversary Adv_1 submits a signcryption query with an input $(PK_{PD_i}, PK_{AP}, m_{PD_i})$ to the challenger $\mathcal{C}$. $\mathcal{C}$ then chooses $r_{PD_i} \in \mathrm{Z}_q^*$ and computes $R_{PD_i} = r_{PD_i} PK_{AP}$. Next, $\mathcal{C}$ computes $b = H_2(R_{PD_i})$ where $H_2(R_{PD_i})$ can be retrieved from list L_{H_2}. Additionally, $\mathcal{C}$ computes $c = b \oplus m_{PD_i}$ and $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$, where $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$ can be retrieved from list L_{H_3}. Finally, $\mathcal{C}$ computes $s = {r_{PD_i}}^{-1}\left(e + SK_{PD_i}\right)$, returns $\varrho_i = (c, e, s)$ to adversary Adv_1 and updates list L_{Sig} with the tuple (c, e, s, ϱ_i).

Unsigncryption query: Adversary Adv_1 submits an unsigncryption query with an input $(PK_{PD_i}, PK_{AP}, \varrho_i)$ to the challenger $\mathcal{C}$. $\mathcal{C}$ computes $y = s^{-1}$ and $V_{AP} = eyPK_{AP} + yPK_{PD_i}SK_{AP}$. If $V_{AP} \notin L_{H_2}$, an error message is returned. Otherwise, $\mathcal{C}$ computes $b' = H_2(V_{AP})$, then $m_{PD_i} = b' \oplus c$. If $(m_{PD_i}, V_{AP}, PK_{PD_i}, PK_{AP}, PID_{PD_i}, t_i) \notin L_{H_3}$, an error message is returned. Otherwise, $\mathcal{C}$ computes $e' = H_3(m_{PD_i}, V_{AP}, PK_{PD_i}, PK_{AP}, PID_{PD_i}, t_i)$. If $e' \neq e$, an error message is returned. Otherwise, $\mathcal{C}$ returns m_{PD_i} to Adv_1 and updates list L_{Unsig} with (m_{PD_i})

Challenge: Adversary Adv_1 gives two challenge plaintexts $\{m_{PD_0}, m_{PD_1}\}$ and a target pseudo-identity PID_i^* to challenger $\mathcal{C}$. Next, $\mathcal{C}$ chooses $i \in \{0,1\}$ at random, $b^* \in \{0,1\}^l$, and $e^*, s^* \in \mathrm{Z}_q^*$. $\mathcal{C}$ computes $c^* = b^* \oplus m_{PD_i}$ and $y^* = (s^*)^{-1}$. $\mathcal{C}$ queries values α_i and β_{PD_i} from list $L_{H_0}$and L_{H_1}, respectively. When Adv_1 submits H_2 query with input $R^*_{PD_i} = (e^*y^* + y^*SK_{PD_i})PK_{AP}$, $\mathcal{C}$ returns b^*. When Adv_1 submits H_3 query with input $(m_{PD_i}, R^*_{PD_i} = (e^*y^* + y^*SK_{PD_i})PK_{AP}, PK_{PD_i}, PK_{AP})$, $\mathcal{C}$ returns e^*. Finally, $\mathcal{C}$ returns ciphertext $\varrho_i^* = (c^*, e^*, s^*)$ to Adv_1.

Phase-II

Adversary Adv_1 can execute all queries in phase-I except unsigncryption query on ϱ_i^* to extract plaintext m_{PD_i}.

Guess: Lastly, Adv_1 makes a guess $i' \in \{0,1\}$ for i. If $i' = i$ holds, adversary Adv_1 returns $r_{PD_i} = ey + ySK_{PD_i}$ as the solution to CDH problem. Otherwise, Adv_1 fails to solve CDH.

Theorem 2: Assume that adversary Adv_2 can win Game 2 with a non-negligible advantage $\mathcal{E}' \geq \frac{\varepsilon}{(q_{H_0}+q_{H_1}+q_{H_2}+q_{H_3}+q_{Sig}+q_{Unsig})}$, in ROM after $q_{H_i}(i = 0, \ldots, 3)$ hash queries, q_{Sig} signcryption query and q_{Uns} unsigncryption query. Then, there exists a challenger $\mathcal{C}$ who can provide solution to CDH problem with a minimum advantage $\mathcal{E}'$ as defined at the proof end.

Proof: Suppose (P, aP, bP) is an instance of CDH problem, where $a, b \in \mathrm{Z}_q^*$. We show how challenger $\mathcal{C}$ in Game 2 interacts with adversary Adv_2 to compute $C = abP$.

Setup: The challenger $\mathcal{C}$ executes this algorithm, which generates the system parameters $params$ as $\{p, q, G, P, PK_{NM}, H_0, H_1, H_2, H_3\}$ and a master private key s_{NM}. Note, the challenger $\mathcal{C}$ shares the $params$ with Adv_2 but keeps s_{NM} a secret. To ensure consistency of the queries and responses to ROM, the challenger $\mathcal{C}$ maintains lists $L_{H_i}(i = 0, \ldots, 3)$ for hash queries, and lists L_{PPK}, L_{SK}, L_{PK}, L_{Sig} and L_{Unsig} for partial private key query, secret key query, public key query, signcryption query, and unsigncryption query, respectively. Note all the lists are initially set to empty.

Phase-I

The challenger $\mathcal{C}$ randomly chooses PID_i^* as the target pseudo identity to be challenged. At this point, the study adopts the irreflexivity assumption i.e., given two pseudo identities PID_1 and PID_2, if $PID_1 = \mathrm{PID}_i^*$, then $PID_2 \neq \mathrm{PID}_i^*$ and vice versa.

H_0 query: Adversary Adv_2 submits a (α_i, T_i) query to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple (α_i, T_i, h_0) from the L_{H_0} list and returns h_0 if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $h_0 \in \mathrm{Z}_q^*$ at random and returns h_0 to Adv_2. Then, challenger $\mathcal{C}$ updates L_{H_0} with tuple (α_i, T_i, h_0).

H_1 query: Adversary Adv_2 submits a query on $(PID_i, D_{PD_i}, PK_{NM})$ to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple $(PID_i, D_{PD_i}, PK_{NM}, \beta_{PD_i})$ from the L_{H_1} list and returns β_{PD_i} if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $\beta_{PD_i} \in Z_q^*$ at random and returns β_{PD_i} to Adv_2. Then, challenger $\mathcal{C}$ updates L_{H_1} with tuple $(PID_i, D_{PD_i}, PK_{NM}, \beta_{PD_i})$.

H_2 query: Adversary Adv_2 submits a query on (R_{PD_i}) to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple (R_{PD_i}, b) from the L_{H_2} list and returns b if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $b \in Z_q^*$ at random and returns b to Adv_2. Then, challenger $\mathcal{C}$ updates L_{H_2} with tuple(R_{PD_i}, b).

H_3 query: Adversary Adv_2 submits a query on $(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$ to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple $(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i, e)$ in the list L_{H_3} and returns e if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $e \in Z_q^*$ at random and returns e to Adv_2. Then, challenger $\mathcal{C}$ updates L_{H_3} with tuple $(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i, e)$.

Partial private key query: Adversary Adv_2 submits a query for the partial private key for PID_{PD_i} to the challenger $\mathcal{C}$. If $PID_i = PID_i^*$, challenger $\mathcal{C}$ terminates the algorithm. Otherwise, if $PID_i \neq PID_i^*$, challenger $\mathcal{C}$ performs the following: selects $\eta_i, \phi_i \in Z_q^*$ at random and computes $D_{PD_i} = \eta_i P - \phi_i P$. Next, challenger $\mathcal{C}$ sets $k_{PD_i} = \eta_i$, $H_1(PID_i, D_{PD_i}, PK_{NM}) = \beta_{PD_i} = \phi_i$ and PPK_{PD_i}=(k_{PD_i}, D_{PD_i}). Finally, Challenger $\mathcal{C}$ returns PPK_{PD_i} to adversary Adv_2 as partial private key and updates list L_{PPK} with the tuple $(PID_i, D_{PD_i}, \beta_{PD_i}, k_{PD_i})$.

Public key query: Adversary Adv_2 submits a query for the public key for PID_i to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for PID_i query in the list L_{PK} and returns PK_{PD_i} if the query exists. Otherwise, $\mathcal{C}$ recovers tuple $(PID_i, D_{PD_i}, \beta_{PD_i}, k_{PD_i})$ from L_{PPK}. Next, $\mathcal{C}$ chooses $x_{PD_i} \in Z_q^*$ at random and computes $X_{PD_i} = x_{PD_i} PK_{NM}$ and $Y_{PD_i} = k_{PD_i} PK_{NM}$. Finally, $\mathcal{C}$ returns $PK_{PD_i} = (X_{PD_i} + Y_{PD_i})$ to Adv_2 as public key and updates list L_{PK} with the tuple $(PID_i, k_{PD_i}, x_{PD_i}, PK_{PD_i})$.

Private key query: Adversary Adv_2 submits a query for the private key for PID_i to the challenger $\mathcal{C}$. If $PID_i = PID_i^*$, $\mathcal{C}$ terminates the algorithm. Otherwise, if $PID_i \neq$

PID_i^*, challenger $\mathcal{C}$ performs the following: searches for PID_i query in the list L_{PK} and returns SK_{PD_i} to Adv_2 if the query exists. Otherwise, $\mathcal{C}$ runs partial private key and public key queries to output tuple $\left(PID_i, k_{PD_i}, x_{PD_i}, X_{PD_i}, Y_{PD_i}\right)$. Finally, $\mathcal{C}$ returns $SK_{PD_i} = (k_{PD_i}, x_{PD_i})$ as Adv_1 as the private key.

Public key replace query: Adversary Adv_2 submits a query for the replacement of public key with an input (PID_i, PK'_{PD_i}) to the challenger $\mathcal{C}$, where $PK'_{PD_i} = X'_{PD_i} + Y'_{PD_i}$, $X'_{PD_i} = x'_{PD_i} PK_{NM}$ and $Y'_{PD_i} = k'_{PD_i} PK_{NM}$. If $PID_i = \text{PID}_i^*$, $\mathcal{C}$ terminates the algorithm since PID_i^* is a target identity. Note Adv_2 cannot ask for public key replace query for target identity. Otherwise, $\mathcal{C}$ sets $X_{PD_i} = X'_{PD_i}$, $Y_{PD_i} = Y'_{PD_i}$, $k_{PD_i} = k'_{PD_i}$ and $x_{PD_i} = x'_{PD_i}$. Finally, $\mathcal{C}$ updates list L_{PK} with the tuple $\left(PID_i, k'_{PD_i}, x'_{PD_i}, PK'_{PD_i}\right)$.

Signcryption query: Adversary Adv_2 submits a signcryption query with an input $(PK_{PD_i}, PK_{AP}, m_{PD_i})$ to the challenger $\mathcal{C}$. $\mathcal{C}$ then chooses $r_{PD_i} \in \mathrm{Z}_q^*$ and computes $R_{PD_i} = r_{PD_i} PK_{AP}$. Next, $\mathcal{C}$ computes $b = H_2(R_{PD_i})$ where $H_2(R_{PD_i})$ can be retrieved from list L_{H_2}. Additionally, $\mathcal{C}$ computes $c = b \oplus m_{PD_i}$ and $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$, where $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$ can be retrieved from list L_{H_3}. Finally, $\mathcal{C}$ computes $s = {r_{PD_i}}^{-1}\left(e + SK_{PD_i}\right)$, returns $\varrho_i = (c, e, s)$ to adversary Adv_2 and updates list L_{Sig} with the tuple (c, e, s, ϱ_i).

Unsigncryption query: Adversary Adv_2 submits an unsigncryption query with an input $(PK_{PD_i}, PK_{AP}, \varrho_i)$ to the challenger $\mathcal{C}$. $\mathcal{C}$ computes $y = s^{-1}$ and $V_{AP} = eyPK_{AP} + yPK_{PD_i} SK_{AP}$. $V_{AP} \notin L_{H_2}$, an error message is returned. Otherwise, $\mathcal{C}$ computes $b' = H_2(V_{AP})$, then $m_{PD_i} = b' \oplus c$. If $(m_{PD_i}, V_{AP}, PK_{PD_i}, PK_{AP}, PID_{PD_i}, t_i) \notin L_{H_3}$, an error message is returned. Otherwise, $\mathcal{C}$ computes $e' = H_3(m_{PD_i}, V_{AP}, PK_{PD_i}, PK_{AP}, PID_{PD_i}, t_i)$. If $e' \neq e$, an error message is returned. Otherwise, $\mathcal{C}$ returns m_{PD_i} to Adv_2 and updates list L_{Unsig} with (m_{PD_i})

Challenge: Adversary Adv_2 gives two challenge plaintexts $\{m_{PD_0}, m_{PD_1}\}$ and a target pseudo-identity PID_i^* to challenger $\mathcal{C}$. Next, $\mathcal{C}$ chooses $i \in \{0,1\}$ at random, $b^* \in \{0,1\}^l$, and $e^*, s^* \in \text{Z}_q^*$. $\mathcal{C}$ computes $c^* = b^* \oplus m_{PD_i}$ and $y^* = (s^*)^{-1}$. $\mathcal{C}$ queries values α_i and β_{PD_i} from list $L_{H_0}$and L_{H_1}, respectively. When Adv_1 submits H_2 query with input $R_{PD_i}^* = (e^*y^* + y^*SK_{PD_i})PK_{AP}$, $\mathcal{C}$ returns b^*. When Adv_2 submits H_3 query with input (m_{PD_i}, $R_{PD_i}^* = (e^*y^* + y^*SK_{PD_i})PK_{AP}$, PK_{PD_i}, PK_{AP}), $\mathcal{C}$ returns e^*. Finally, $\mathcal{C}$ returns ciphertext $\varrho_i^* = (c^*, e^*, s^*)$ to Adv_2.

Phase-II

Adversary Adv_2 can execute all queries in phase-I except unsigncryption query on ϱ_i^* to extract plaintext m_{PD_i}.

Guess: Lastly, Adv_2 makes a guess $i' \in \{0,1\}$ for i. If $i' = i$ holds, adversary Adv_2 returns $r_{PD_i} = ey + ySK_{PD_i}$ as the solution to CDH problem. Otherwise, Adv_2 fails to solve CDH.

Definition 1: The proposed scheme is IND-CCA if an adversary has negligible advantage of winning games 1 and 2 under a polynomial time-bound algorithm.

4.3.1.2. Unforgeability

As earlier mentioned, the proposed signcryption scheme combines digital signature and encryption techniques in a single logical step. For digital signature, unforgeability is required to ensure no external party can generate a valid signature without access to necessary parameters. We use theorem 3 and 4 to prove unforgeability of the proposed scheme.

Theorem 3: Assume that adversary Adv_1 can win Game 3 with a non-negligible advantage $\mathcal{E}' \geq \frac{\varepsilon}{(q_{H_0}+q_{H_1}+q_{H_2}+q_{H_3}+q_{Sig})}$, in ROM after $q_{H_i}(i = 0, \ldots, 3)$ hash queries, and q_{Sig} signcryption query. Then, there is a challenger $\mathcal{C}$ in existence who can compute the ECDL problem with a minimum advantage $\mathcal{E}'$ as defined at the proof end.

Proof: Suppose $(Q = aP)$ is a case of ECDL problem, where $a \in \text{Z}_q^*$. We show how challenger $\mathcal{C}$ in Game 1 interacts with adversary Adv_1 to compute a from Q and P

Setup: The challenger $\mathcal{C}$ executes this algorithm, which generates the system parameters $params$ as $\{p, q, G, P, PK_{NM}, H_0, H_1, H_2, H_3\}$ and a master private key s_{NM}. Note, the challenger $\mathcal{C}$ shares the $params$ with Adv_1 but keeps s_{NM} a secret. To ensure consistency of the queries and responses to ROM, the challenger $\mathcal{C}$ maintains lists $L_{H_i}(i = 0, \ldots, 3)$ for hash queries, and lists L_{PPK}, L_{SK}, L_{PK}, L_{Sig} and L_{Unsig} for partial private key query, secret key query, public key query, signcryption query, and unsigncryption query, respectively. Note all the lists are initially set to empty.

Phase-I

The challenger $\mathcal{C}$ randomly chooses PID_i^* as the target pseudo identity to be challenged. At this point, the study adopts the irreflexivity assumption (A. A. O. Li, 2018), i.e., given two pseudo identities PID_1 and PID_2, if $PID_1 = \text{PID}_i^*$, then $PID_2 \neq \text{PID}_i^*$ and vice versa.

H_0 query: Adversary Adv_1 submits a (α_i, T_i) query to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple (α_i, T_i, h_0) from the L_{H_0} list and returns h_0 if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $h_0 \in \text{Z}_q^*$ at random and returns h_0 to Adv_1. Then, challenger $\mathcal{C}$ updates L_{H_0} with tuple (α_i, T_i, h_0).

H_1 query: Adversary Adv_1 submits a query on $(PID_i, D_{PD_i}, PK_{NM})$ to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple $(PID_i, D_{PD_i}, PK_{NM}, \beta_{PD_i})$ from the L_{H_1} list and returns β_{PD_i} if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $\beta_{PD_i} \in \text{Z}_q^*$ at random and returns β_{PD_i} to Adv_1. Then, challenger $\mathcal{C}$ updates L_{H_1} with tuple $(PID_i, D_{PD_i}, PK_{NM}, \beta_{PD_i})$.

H_2 query: Adversary Adv_1 submits a query on (R_{PD_i}) to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple (R_{PD_i}, b) from the L_{H_2} list and returns b if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $b \in \text{Z}_q^*$ at random and returns b to Adv_1. Then, challenger $\mathcal{C}$ updates L_{H_2} with tuple(R_{PD_i}, b).

H_3 query: Adversary Adv_1 submits a query on $\left(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i\right)$ to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple $\left(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i, e\right)$ from the L_{H_3} list and returns e if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $e \in \text{Z}_q^*$ at random and returns e to Adv_1. Then, challenger $\mathcal{C}$ updates L_{H_3} with tuple $\left(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i, e\right)$.

Partial private key query: Adversary Adv_1 submits a query for the partial private key for PID_{PD_i} to the challenger $\mathcal{C}$. If $PID_i = \text{PID}_i^*$, challenger $\mathcal{C}$ terminates the algorithm. Otherwise, if $PID_i \neq \text{PID}_i^*$, challenger $\mathcal{C}$ performs the following: selects $\eta_i, \phi_i \in \text{Z}_q^*$ at random and computes $D_{PD_i} = \eta_i P - \phi_i P$. Next, challenger $\mathcal{C}$ sets $k_{PD_i} = \eta_i$, $H_1(PID_i, D_{PD_i}, PK_{NM}) = \beta_{PD_i} = \phi_i$ and PPK_{PD_i}=(k_{PD_i}, D_{PD_i}). Finally, Challenger $\mathcal{C}$ returns PPK_{PD_i} to adversary Adv_1 as partial private key and updates list L_{PPK} with the tuple $(PID_i, D_{PD_i}, \beta_{PD_i}, k_{PD_i})$.

Private key query: Adversary Adv_1 submits a query for private key for PID_i to the challenger $\mathcal{C}$. If $PID_i = \text{PID}_i^*$, $\mathcal{C}$ terminates the algorithm. Otherwise, if $PID_i \neq \text{PID}_i^*$, challenger $\mathcal{C}$ performs the following: searches for PID_i query in the list L_{PK} and returns SK_{PD_i} to Adv_1 if the query exists. Otherwise, $\mathcal{C}$ runs partial private key and public key queries to output tuple $(PID_i, k_{PD_i}, x_{PD_i}, X_{PD_i}, Y_{PD_i})$. Finally, $\mathcal{C}$ returns $SK_{PD_i} = (k_{PD_i}, x_{PD_i})$ to Adv_1 as the private key.

Public key query: Adversary Adv_1 submits a query for public key for PID_i to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for PID_i query in the list L_{PK} and returns PK_{PD_i} if the query exists. Otherwise, $\mathcal{C}$ recovers tuple $(PID_i, D_{PD_i}, \beta_{PD_i}, k_{PD_i})$ from L_{PPK}. Next, $\mathcal{C}$ chooses $x_{PD_i} \in \text{Z}_q^*$ at random and computes $X_{PD_i} = x_{PD_i} PK_{NM}$ and $Y_{PD_i} = k_{PD_i} PK_{NM}$. Finally, $\mathcal{C}$ returns $PK_{PD_i} = (X_{PD_i} + Y_{PD_i})$ to Adv_1 as public key and updates list L_{PK} with the tuple $(PID_i, k_{PD_i}, x_{PD_i}, PK_{PD_i})$.

Signcryption query: Adversary Adv_1 submits a signcryption query with an input $(PK_{PD_i}, PK_{AP}, m_{PD_i})$ to the challenger $\mathcal{C}$. $\mathcal{C}$ then chooses $r_{PD_i} \in \text{Z}_q^*$ and computes $R_{PD_i} = r_{PD_i} PK_{AP}$. Next, $\mathcal{C}$ computes $b = H_2(R_{PD_i})$ where $H_2(R_{PD_i})$ can be retrieved from list L_{H_2}. Additionally, $\mathcal{C}$ computes $c = b \oplus m_{PD_i}$ and $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$, where $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$ can be retrieved from list L_{H_3}. Finally, $\mathcal{C}$ computes $s = {r_{PD_i}}^{-1}(e + SK_{PD_i})$, returns $\varrho_i = (c, e, s)$ to adversary Adv_1 and updates list L_{Sig} with the tuple (c, e, s, ϱ_i).

Forgery: After all the queries have been made, adversary Adv_1 furnishes challenging pseudo identity PID_i^* i.e., the sender's identity, a message m_{PD}^*, and a challenge

signcryption $\varrho_i^* = (c^* e^* s^*)$. Note, the adversary is forbidden from making unsigncryption query for ϱ_i^* using the target identity's private key as this will result to game termination. Otherwise, the challenger $\mathcal{C}$ outputs a message m as the result for unsigncryption with input $(PK_{PD_i}, PK_{AP}, \varrho_i)$. If $m = m_{PD}^*$ and Adv_1 did not query for PID_i^* private key and neither did adv_1 submit a replace the public key query for PID_i^* nor did adv_1 issue an extract partial private key query for PID_i^* at some point, the adversary Adv_1 wins the game.

Theorem 4: Assume that adversary Adv_2 can win Game 4 with a non-negligible advantage $\mathcal{E}' \geq \frac{\varepsilon}{(q_{H_0}+q_{H_1}+q_{H_2}+q_{H_3}+q_{Sig})}$, in ROM after $q_{H_i}(i = 0, \ldots, 3)$ hash queries, and q_{Sig} signcryption query. Then, there is a challenger $\mathcal{C}$ in existence, who can compute the ECDL problem with a minimum advantage $\mathcal{E}'$ as defined at the proof end.

Proof: Suppose $(Q = aP)$ is a case of ECDL problem, where $a \in \mathrm{Z}_q^*$. We show how challenger $\mathcal{C}$ in Game 2 interacts with adversary Adv_2 to compute a from Q and P

Setup: The challenger $\mathcal{C}$ executes this algorithm, which generates the system parameters $params$ as $\{p, q, G, P, PK_{NM}, H_0, H_1, H_2, H_3\}$ and a master private key s_{NM}. Note, the challenger $\mathcal{C}$ shares the $params$ with Adv_2 but keeps s_{NM} a secret. To ensure consistency of the queries and responses to ROM, the challenger $\mathcal{C}$ maintains lists $L_{H_i}(i = 0, \ldots, 3)$ for hash queries, and lists L_{PPK}, L_{SK}, L_{PK}, L_{Sig} and L_{Unsig} for partial private key query, secret key query, public key query, signcryption query, and unsigncryption query, respectively. Note all the lists are initially set to empty.

Phase-I

The challenger $\mathcal{C}$ randomly chooses PID_i^* as the target pseudo identity to be challenged. At this point, the study adopts the irreflexivity assumption i.e., given two pseudo identities PID_1 and PID_2, if $PID_1 = \mathrm{PID}_i^*$, then $PID_2 \neq \mathrm{PID}_i^*$ and vice versa.

H_0 query: Adversary Adv_1 submits a (α_i, T_i) query to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple (α_i, T_i, h_0) in the L_{H_0} list and returns h_0 if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $h_0 \in \mathrm{Z}_q^*$ at random and returns h_0 to Adv_2. Then, challenger $\mathcal{C}$ updates L_{H_0} with tuple (α_i, T_i, h_0).

H_1 query: Adversary Adv_2 submits a query on $(PID_i, D_{PD_i}, PK_{NM})$ to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple $(PID_i, D_{PD_i}, PK_{NM}, \beta_{PD_i})$ in the L_{H_1} list and returns β_{PD_i} if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $\beta_{PD_i} \in Z_q^*$ at random and returns β_{PD_i} to Adv_2. Then, challenger $\mathcal{C}$ updates L_{H_1} with tuple $(PID_i, D_{PD_i}, PK_{NM}, \beta_{PD_i})$.

H_2 query: Adversary Adv_2 submits a query on (R_{PD_i}) to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple (R_{PD_i}, b) in the L_{H_2} list and returns b if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $b \in Z_q^*$ at random and returns b to Adv_2. Then, challenger $\mathcal{C}$ updates L_{H_2} with tuple(R_{PD_i}, b).

H_3 query: Adversary Adv_2 submits a query on $(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$ to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple $(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i, e)$ in the L_{H_3} list and returns e if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $e \in Z_q^*$ at random and returns e to Adv_2. Then, challenger $\mathcal{C}$ updates L_{H_3} with tuple $(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i, e)$.

Partial private key query: Adversary Adv_2 submits a query for partial private key for PID_{PD_i} to the challenger $\mathcal{C}$. If $PID_i = PID_i^*$, challenger $\mathcal{C}$ terminates the algorithm. Otherwise, if $PID_i \neq PID_i^*$, challenger $\mathcal{C}$ performs the following: selects $\eta_i, \phi_i \in Z_q^*$ at random and computes $D_{PD_i} = \eta_i P - \phi_i P$. Next, challenger $\mathcal{C}$ sets $k_{PD_i} = \eta_i$, $H_1(PID_i, D_{PD_i}, PK_{NM}) = \beta_{PD_i} = \phi_i$ and PPK_{PD_i}=(k_{PD_i}, D_{PD_i}). Finally, Challenger $\mathcal{C}$ returns PPK_{PD_i} to adversary Adv_2 as partial private key and updates list L_{PPK} with the tuple $(PID_i, D_{PD_i}, \beta_{PD_i}, k_{PD_i})$.

Private key query: Adversary Adv_2 submits a query for private key for PID_i to the challenger $\mathcal{C}$. If $PID_i = PID_i^*$, $\mathcal{C}$ terminates the algorithm. Otherwise, if $PID_i \neq PID_i^*$, challenger $\mathcal{C}$ performs the following: searches for PID_i query in the list L_{PK} and returns SK_{PD_i} to Adv_2 if the query exists. Otherwise, $\mathcal{C}$ runs partial private key and public key queries to output tuple $(PID_i, k_{PD_i}, x_{PD_i}, X_{PD_i}, Y_{PD_i})$. Finally, $\mathcal{C}$ returns $SK_{PD_i} = (k_{PD_i}, x_{PD_i})$ to Adv_2 as the private key.

Public key query: Adversary Adv_2 submits a query for public key for PID_i to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for PID_i query in the list L_{PK} and returns PK_{PD_i} if the

query exists. Otherwise, $\mathcal{C}$ recovers tuple $\left(PID_i, D_{PD_i}, \beta_{PD_i}, k_{PD_i}\right)$ from L_{PPK}. Next, $\mathcal{C}$ chooses $x_{PD_i} \in Z_q^*$ at random and computes $X_{PD_i} = x_{PD_i} PK_{NM}$ and $Y_{PD_i} = k_{PD_i} PK_{NM}$. Finally, $\mathcal{C}$ returns $PK_{PD_i} = (X_{PD_i} + Y_{PD_i})$ to Adv_2 as public key and updates list L_{PK} with the tuple $\left(PID_i, k_{PD_i}, x_{PD_i}, PK_{PD_i}\right)$.

Signcryption query: Adversary Adv_2 submits a signcryption query with an input $(PK_{PD_i}, PK_{AP}, m_{PD_i})$ to the challenger $\mathcal{C}$. $\mathcal{C}$ then chooses $r_{PD_i} \in Z_q^*$ and computes $R_{PD_i} = r_{PD_i} PK_{AP}$. Next, $\mathcal{C}$ computes $b = H_2(R_{PD_i})$ where $H_2(R_{PD_i})$ can be retrieved from list L_{H_2}. Additionally, $\mathcal{C}$ computes $c = b \oplus m_{PD_i}$ and $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$, where $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$ can be retrieved from list L_{H_3}. Finally, $\mathcal{C}$ computes $s = {r_{PD_i}}^{-1}\left(e + SK_{PD_i}\right)$, returns $\varrho_i = (c, e, s)$ to adversary Adv_2 and updates list L_{Sig} with the tuple (c, e, s, ϱ_i).

Forgery: After all the queries have been made, adversary Adv_2 furnishes challenging pseudo identity PID_i^* i.e., the sender's identity, a message m_{PD}^*, and a challenge signcryption $\varrho_i^* = (c^* e^* s^*)$.

Note that the adversary is forbidden from making unsigncryption query for ϱ_i^* using the target identity's private key as this will result to game termination. Otherwise, the challenger $\mathcal{C}$ outputs a message m as the result of unsigncryption with input $(PK_{PD_i}, PK_{AP}, \varrho_i)$. If $m = m_{PD}^*$ and Adv_2 did not query for PID_i^* private key or issue an extract partial private key query for PID_i^* at some point, the adversary Adv_2 wins the game.

Definition 2: The proposed scheme is EUF-CMA if an adversary has a negligible advantage in winning games 3 and 4 under a polynomial time-bound algorithm.

4.3.2. Informal Security Analysis

This section conducts a security analysis to demonstrate that the scheme proposed in this study meets the required security features outlined in Section 3.5.2.

4.3.2.1. Authentication (Sender and Message)

Sender Authentication

Sender authentication allows the recipient to verify the validity of the sending device. It prevents a malicious device from sending messages that would compromise the patient's safety. During the registration of entities, each entity must submit its real identity to the NM for scrutiny. The patient's device (PD) thus submits its identity RID_{PD_i}. If the real identity is found missing in the manufacturer's database, it is discarded. Otherwise, the NM uses its master private key s_{NM} to generate the pseudo-identity of the patient device (PD). Further, it attaches a validity period T_i to the pseudo-identity before submitting the tuple $PID_i = \{PID_{i1}, PID_{i2}, T_i\}$ to PD. The receiving entity i.e., the Application Provider (AP) therefore verifies the validity of the PD using the attached validity period T_i and pseudo-identity PID_i. Besides, the fact that the real identities of entities were authenticated during registration and the NM's master private key s_{NM} is difficult to compute as a result of the hardness of ECDLP makes it hard for an attacker to forge a valid PID. This therefore ensures that the sender's authenticity is verified.

Message Authentication

Message authentication allows the recipient to check whether the received message has been tampered with. Before accepting the message, the AP has to verify it by extracting the message timestamp t_i attached to the message and checking its expiration. Using the PD's public key and the AP's private key, the AP further runs an unsigncryption algorithm. The capability of obtaining the correct plaintext, together with the freshness of the message guarantees the validity of the received message. Additionally, the scheme proposed is EUF-CMA secure against type I and II adversaries. Forging a valid signcryption that will pass the unsigncryption equation $V_{AP} = eyPK_{AP} + yPK_{PD_i}SK_{AP}$ implies that there is an adversary in existence, who can solve ECDLP with a non-negligible advantage. According to security proof of unforgeability, there is no such adversary. Consequently, proposed scheme possesses message authentication.

4.3.2.2. Confidentiality

Confidentiality ensures the patient's data remains private and inaccessible to unauthorized users. The proposed signcryption scheme combines digital signature and encryption techniques in a single logical step. The encryption property is responsible for confidentiality, i.e., on input of a health-related message $m_{PD_i} \in \{0,1\}^*$, system parameters $params$, pseudo-identity $PID_{PD_i,}$ private key SK_{PD_i}, and AP's public key PK_{AP}, the PD outputs a signcrypted message ϱ_i for transmission. For the AP to obtain the message's details, it is must provide a private key that matches with the PD's public key. Besides, proposed scheme is IND-CCA secure against Adv_1 and Adv_2. The scheme, therefore, has confidentiality.

4.3.2.3. Unforgeability

Unforgeability is a security requirement meant to prevent a malicious user from generating a valid signature using a valid private key. To access the private key used to generate a valid signature, the attacker must solve the ECDL problem, which is intractable. From security proof on unforgeability, the proposed scheme is EUF-CMA secure against Adv_1 and Adv_2. Therefore, the scheme, has unforgeability.

4.3.2.4. Non-repudiation

Non-repudiation ensures that a party does not deny having sent a message or performed an action, i.e., if a sender signcrypts a message utilizing her private key, they cannot later deny to have signed. In the proposed scheme, during signcryption, the PD uses its private key SK_{PD_i} to sign the message (i.e., calculate the hash value) with the corresponding AP's public key PK_{AP}. Besides, the AP on the other hand uses its private key SK_{AP} and the corresponding PD's public key PK_{PD_i} to unsigncrypt the message (i.e., calculate the hash value). If the received and computed hash values are comparable, then the sender undeniably signed the message. Therefore, proposed scheme has non-repudiation.

4.3.2.5. Key-escrow Resistance

Key escrow is a security problem involving a trusted third party in a network having access to the full private keys of communicating entities, thus exposing the party to the risk of being compromised to generate valid signatures on messages. The scheme proposed in this

study is resilient to key escrow issue. During registration and key generation, the Network Manager (NM), which is the trusted third party, generates a pseudo-identity $PID_i = \{PID_{i1}, PID_{i2}, T_i\}$ and partial private key $PPK_{PD_i}=\{k_{PD_i}, D_{PD_i}\}$ for the PD whose registration is being sought. Meanwhile, PD uses the partial private key to compute its full private key as $PK_{PD_i} = (X_{PD_i}, Y_{PD_i})$. Thus, the NM has no idea of the full private key of the PD. This renders the proposed scheme Key-escrow resistant.

4.3.2.6. Availability

The availability property ensures that all permitted entities can access to resources at any time they require them. The proposed scheme provides an authentication mechanism to allow the recipient of the message, i.e., the AP, for instance, to use its private key and the corresponding PD's public key to unsigncrypt the received signcryption and vice versa. This ensures that any entity with the required set of keys can access resources as and when needed. The scheme therefore achieves availability.

4.3.2.7. Forward Secrecy

Forward secrecy, commonly referred to as perfect forward secrecy (PFS), is a property assures that the confidentiality of earlier signed messages is not compromised in the event that the sender's private key gets leaked. In the proposed scheme, in the event of the exposure of the sender's private key, it is required that any attacker intending to read the content of the previous signcryption obtain the value of b, which requires for yet another randomly selected value r_{PD_i}. Obtaining r_{PD_i} implies that the attacker is able to solve the ECDL problem, a problem believed to be intractable. Furthermore, the random value r_{PD_i} keeps changing when there is new communication, so it cannot be used to reveal the details of earlier communication. The scheme therefore has perfect forward secrecy.

4.3.2.8. Conditional Anonymity

In conditional anonymity, the real identities of users remain concealed but may be revealed by a trusted authority under certain circumstances, for example, when an entity denies a misbehavior or is involved in a dispute emanating from a malicious act. According to proposed protocol, the PDs must register by submitting their real identities to the network manager (NM). Next, the NM generates the corresponding pseudo-identity PID_i upon

scrutinizing the real identity. This step involves the NM computing the hash value of its master key s_{NM} alongside the PD's real identity, i.e., $RID_{PD_i} = PID_{i2} \oplus H_0(s_{NM} PID_{i1})$. In the event that an attacker obtains a pseudo-identity $PID_i = \{PID_{i1}, PID_{i2}, T_i\}$, it is impossible to retrieve the real identity of the PD following the hardness of ECDLP and the characteristics of hash functions.

4.3.2.9. Resistance to Common Attacks

Replay attacks

A replay attack entails an attacker maliciously intercepting and retransmitting a previously exchanged valid message. In the proposed scheme, the signcryption $\varrho_i = (c, e, s)$ has a timestamp t_i, i.e., $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$, which the receiver has to verify the freshness of the message. The message is rejected if it is found to be expired.

Message falsification attacks

In message falsification attack, an adversary attempts to alter, without detection, the content of a signcrypted message. The proposed scheme has confidentiality, which makes the scheme secure against message falsification attacks.

Impersonation attacks

An impersonation attack involves an attacker representing themselves falsely as legitimate users, usually the sender, and consequently leading the recipient into believing that the received forged signature is authentic. In the proposed scheme, any attacker intending to impersonate must run the signcryption algorithm successfully, which is hard under ECDLP as informally discussed in Section 2.2.4. Additionally, recipient must verify the sender's authenticity by checking the freshness of the validity time period T_i attached to the pseudo-identity of the sender, i.e., $PID_i = \{PID_{i1}, PID_{i2}, T_i\}$. Besides, during key generation, the NM generates partial private keys for entities, which further generate their full private keys. NM therefore cannot access the full private keys of these entities. In the event that NM becomes compromised, it is impossible to impersonate a legal sender.

MITM attacks

From security proof on unforgeability, the proposed scheme is EUF-CMA secure against type I and II adversaries. Consequently, the scheme is resistant to man-in-the-middle attacks.

4.4. Performance Analysis

In this section, the study evaluates the performance of the proposed Secure and Efficient Certificateless Signcryption Protocol (SECSP) in terms of security features, computational cost, and communication cost. The proposed protocol is then compared with the protocols in (Xiong et al., 2022), (Zhou, 2019a), (Liu et al., 2020), (Ullah, Alkhalifah, et al., 2021), (Ramadan et al., 2023), and (Zhang et al., 2024) to demonstrate its effectiveness for application in WBANs.

4.4.1. Security Features

Table 4.2 presents a summary of the security features achieved by the study's scheme and a comparison with other related schemes. The security features considered include: sender authentication, message authentication, confidentiality, unforgeability, non-repudiation, key-escrow resistance, availability, forward secrecy, and conditional anonymity. The study uses the symbols √ to denote that the scheme meets the security property. On contrary, the symbol × denotes that the scheme fails to meet the security property. Notably, the study's scheme meets all the security properties aforementioned, whereas the other six schemes lack various security features, as shown in Table 4.2.

Table 4.2

Comparison of Security Features

Security Feature	Xiong et al. 2022	Zhou 2019	Liu et al. 2020	Ullah et al. 2021	Ramadan et al. 2023	Zhang et al. 2024	Proposed
Sender authentication	×	√	×	×	×	√	√
Message authentication	√	√	√	√	√	√	√
Confidentiality	√	√	√	√	√	√	√
Unforgeability	√	√	×	√	√	√	√
Non-repudiation	√	√	√	√	√	√	√
Key-escrow resistance	×	√	√	√	×	√	√
Availability	√	√	√	√	√	√	√
Forward secrecy	√	√	×	√	√	√	√
Conditional anonymity	×	×	×	√	×	×	√
Approach	PKI-IBC	CLC	CLC	CLC	IBC	CLC	CLC

4.4.2. Computation Cost

Computation cost refers to the amount of resources needed to execute cryptographic operations. It includes the processing time and energy consumption needed for signcryption and unsigncryption. The proposed protocol evaluates the computational cost for both signcryption and unsigncryption algorithms in the proposed SECSP by considering the runtime of the following cryptographic operations: elliptic curve based scalar multiplication, bilinear pairing based scalar multiplication, elliptic curve based point addition, bilinear pairing based point addition, modular inverse, hash function operation, bilinear pairing, and exponentiation, denoted as T_{SM_ecc}, T_{SM_bp}, T_{PA_ecc}, T_{PA_bp}, T_{IN}, T_h, T_{Bp}, and T_{exp}, respectively.

To obtain the running times for the above-mentioned operations, the study conducted a simulation experiment on various cryptographic operations and the results were presented in table 4.3 below. The experiment employed MIRACL CC, a widely recognized encryption

toolkit used for conducting various cryptographic operations across different environments. The results were obtained from a set-up with the following specifications: an Intel i7 processor, Windows 10 operating system, 8GB RAM capacity, and a 3.40 GHz CPU.

Table 4.3

Cryptographic Operations Running Times

Notation	Cryptographic Operation	Run Time (ms)
$\boldsymbol{T_{SM\_ecc}}$	Elliptic Curve Scalar Multiplication	0.442
$\boldsymbol{T_{SM\_bp}}$	Bilinear Pairing Scalar Multiplication	1.709
$\boldsymbol{T_{PA\_ecc}}$	Elliptic Curve Point Addition	0.0018
$\boldsymbol{T_{PA\_bp}}$	Bilinear Pairing Point Addition	0.071
$\boldsymbol{T_{IN}}$	Inverse	0.174
$\boldsymbol{T_{h}}$	General Hash Function	0.0001
$\boldsymbol{T_{Bp}}$	Bilinear Pairing	4.211
$\boldsymbol{T_{exp}}$	Exponentiation	3.886

Table 4.4 presents a summary of the computation costs for the proposed scheme and other related schemes for signcryption and unsigncryption algorithms. From the summary, the computation costs for signcryption and unsigncryption algorithms for the proposed scheme are T_{SM_ecc}+T_{PA_ecc}+T_{IN}+$2T_h = 0.618$ ms and $2T_{SM\_ecc} + T_{PA\_ecc} + T_{IN} + 2T_h = 1.06$ ms, respectively, and the overall computation cost is 1.678 ms. We note that the proposed scheme outperforms the other six related schemes in terms of computational efficiency for both signcryption and unsigncryption algorithms, as well as overall efficiency. In Xiong et al. (2022), the computation cost for signcryption and unsigncryption algorithms is $4T_{SM\_bp} + 4T_h + 2T_{exp} = 14.6084\ ms$ and $3T_{Bp} + T_{PA\_bp} + 5T_h + T_{IN} + T_{exp} = 16.7645\ ms$, respectively, and the overall computation cost is 31.3729 ms. Similarly, the total computation cost in Zhou's scheme (Zhou, 2019a) for the signcryption and unsigncryption algorithms is $5T_{SM\_ecc} + 4T_{PA\_ecc} + 5T_h = 2.2177\ ms$ and $7T_{SM\_ecc} + 4T_{PA\_ecc} + 5T_h = 3.1017\ ms$, respectively, and the overall computation cost is 5.3194 ms. In the same way, for the scheme in Liu et al. (2020), the computational cost is $T_{SM\_bp} + 5T_h + 3T_{IN} + 6T_{exp} = 25.5295\ ms$ and T_{SM_bp}+$3T_h$+T_{IN}+$6T_{exp} = 25.1993$ ms for the signcryption and unsigncryption algorithms respectively. Thus, the overall computational

cost is 50.7288 ms. Likewise, in Ullah et al. (2021), the scheme presented costs $4T_{SM\_ecc}$+$3T_h = 1.7683$ ms for the signcryption algorithm, $4T_{SM\_ecc}$+$3T_h = 1.7683$ ms for the unsigncryption algorithm, and 3.5366 ms for the total computation cost. In the same way, the total computational cost for the scheme in Ramadan et al. (2023) is $2T_{SM\_bp}$+T_{PA_bp}+$4T_h$+$2T_{exp} = 11.4944$ ms and $4T_{Bp}$+T_h=16.4401 ms for the signcryption and unsigncryption algorithms, respectively. The scheme's overall computational cost is 27.9345 ms. Finally, the signcryption and unsigncryption computation costs for the scheme presented in Zhang et al. (2024) are given as $3T_{SM\_ecc}$+$4T_{PA\_ecc}$+$6T_h = 1.3338$ ms and $4T_{SM\_ecc}$+$4T_{PA\_ecc}$+$2T_h = 1.7754$ ms, respectively, and the overall computation cost for the scheme is 3.1092 ms.

The proposed scheme improves the overall computational efficiency against other related schemes as follows: In Xiong et al.'s scheme, efficiency improvement is given as $\frac{31.3729-1.678}{31.3729} \times 100 = 94.64\%$. Likewise, the computational efficiency improvement in Zhou's scheme is computed as follows: $\frac{5.3194-1.678}{5.3194} \times 100 = 68.46\%$. Similarly, efficiency improvement in Liu et al.'s scheme is given as $\frac{50.7288-1.678}{50.7288} \times 100 = 96.69\%$. The computational efficiency improvement in Ullah et al.'s scheme is calculated as follows: $\frac{3.5366-1.678}{3.5366} \times 100 = 52.55\%$. In the same way, efficiency improvement in Ramadan et al.'s scheme is computed as follows: $\frac{27.9345-1.678}{27.9345} \times 100 = 93.99\%$. Finally, the overall efficiency improvement in Zhang et al.'s scheme is given as follows: $\frac{3.1092-1.678}{3.1092} \times 100 = 46.03\%$.

Table 4.4

Computation Cost

Scheme	Signcryption cost (milliseconds)	Unsigncryption cost (milliseconds)	Total cost (milliseconds)
(Xiong et al., 2022)	$4T_{SM\_bp}$+$4T_h$+$2T_{exp}$ =14.6084	$3T_{Bp}$+T_{PA_bp} + $5T_h$ + T_{IN} + T_{exp} = 16.7645	31.3729
(Zhou, 2019a)	$5T_{SM\_ecc}$+$4T_{PA\_ecc}$ + $5T_h$ = 2.2177	$7T_{SM\_ecc}$+$4T_{PA\_ecc}$+$5T_h$ = 3.1017	5.3194
(Liu et al., 2020)	T_{SM_bp}+$5T_h$+$3T_{IN}$+$6T_{exp}$ = 25.5295	T_{SM_bp}+$3T_h$+T_{IN}+$6T_{exp}$ = 25.1993	50.7288
(Ullah, Alkhalifah, et al., 2021)	$4T_{SM\_ecc}$+$3T_h$ = 1.7683	$4T_{SM\_ecc}$+$3T_h$ = 1.7683	3.5366
(Ramadan et al., 2023)	$2T_{SM\_bp}$+T_{PA_bp}+$4T_h$+$2T_{exp}$ = 11.4944	$4T_{Bp}$+T_h=16.4401	27.9345
(Zhang et al., 2024)	$3T_{SM\_ecc}$+$4T_{PA\_ecc}$+$6T_h$ = 1.3338	$4T_{SM\_ecc}$+$4T_{PA\_ecc}$+$2T_h$ = 1.7754	3.1092
Proposed	T_{SM_ecc}+T_{PA_ecc}+T_{IN}+$2T_h$ = 0.618	$2T_{SM\_ecc}$+T_{PA_ecc}+T_{IN}+$2T_h$ = 1.06	1.678

Table 4.5

Efficiency Improvement (%) of the Proposed Scheme over Related Schemes

Scheme	Signcryption	Unsigncryption	Overall
Xiong et al.	95.77%	93.68%	94.65%
Zhou	72.13%	65.83%	68.46%
Liu et al.	97.58%	95.79%	96.69%
Ullah et al.	65.05%	40.06%	52.55%
Ramadan et al.	94.62%	93.55%	93.99%
Zhang et al.	53.67%	40.30%	46.03%

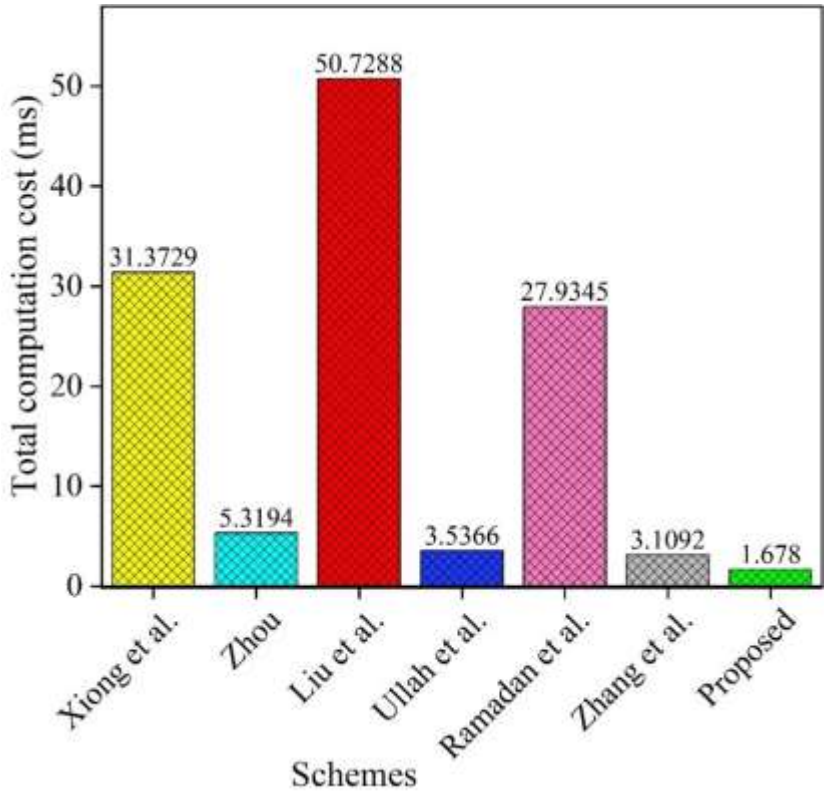

Figure 4.3: Total Computation Cost

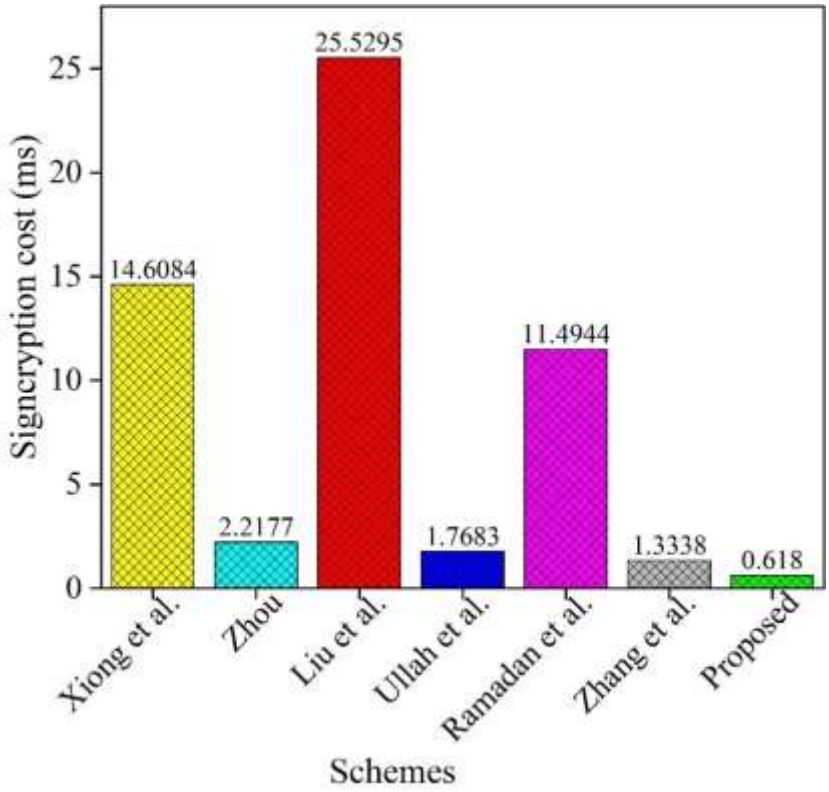

Figure 4.4: Computation Cost for Signcryption

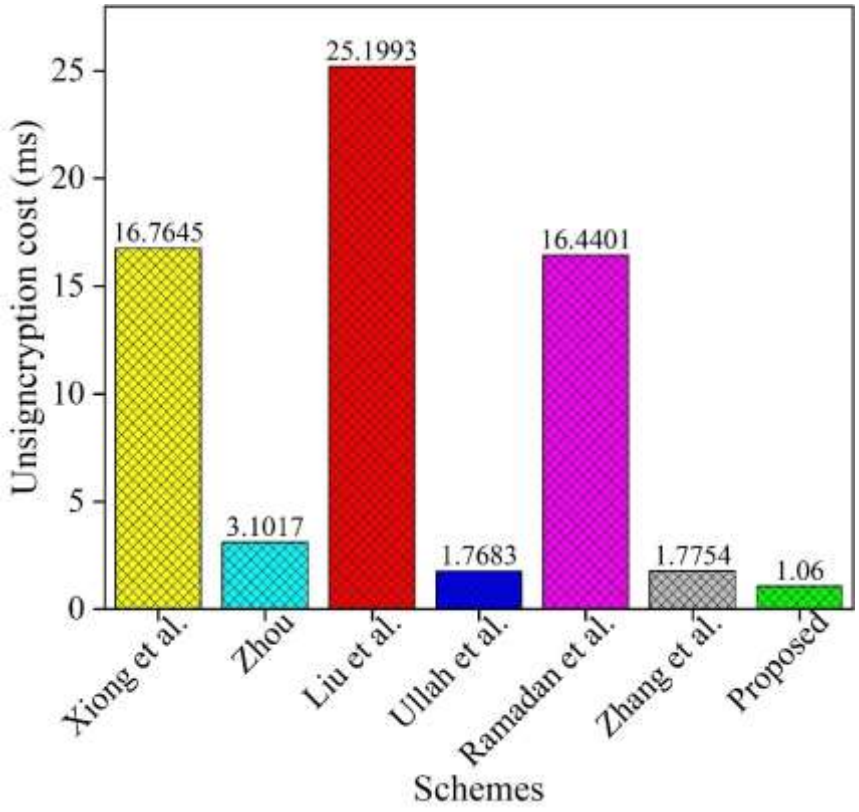

Figure 4.5: Computation Cost for Unsigncryption

4.4.3. Communication Cost

Communication cost refers to the amount of data transmitted between the communicating devices in WABNs. To evaluate the proposed SECSP scheme in terms of communication cost, the study takes into account the cost associated with transmitting ciphertext, the sender's public key, the receiver's public key, and the timestamp, measured in terms of byte size. The proposed scheme is compared with schemes in (Xiong et al., 2022), (Zhou, 2019a), (Liu et al., 2020), (Ullah, Alkhalifah, et al., 2021), (Ramadan et al., 2023), and (Zhang et al., 2024), based on the afore-mentioned parameters. For the analysis of bilinear pairing-based schemes, the study adopts a curve Ê: $y^2 = x^3 + x$ $(mod$ ṕ$)$, and ṕ is a prime number of size 64 bytes. Curve Ê contains some points generated by Ṕ which forms an additive group $\mathbb{G}_1$ with order q , a 20-byte prime number. A bilinear pairing operation is thus defined as $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, $\mathbb{G}_1$ and $\mathbb{G}_2$ being the additive and multiplicative groups respectively. Therefore, the length of $\mathbb{G}_1$ is taken as 128 bytes and that of Z_q^* as 20 bytes. For analysis of elliptic curve-based schemes, the study adopts a curve E: $y^2 = x^3 + ax + b$ $(mod\ p)$, and $p \in Z_q^*$ is a prime number of size 20 bytes. Curve E contains some points

generated by P, which forms a cyclic additive group $\mathbb{G}$ of order q, where $q \in Z_q^*$ is a 20-byte prime number. Therefore, the length of $|\mathbb{G}_1|$ is taken as 40 bytes and that of $|Z_q^*|$ as 20 bytes. The length of the plaintext message $|m|$ and timestamp $|t|$ are assumed to be 20 bytes and 4 bytes, respectively, for both bilinear pairing and elliptic curve-based schemes. Table 4.6 provides a summary of the above-mentioned parameters and their respective byte lengths.

Tabe 4.6

Summary of Byte Length of Parameters

Nature of the Curve	Length of Element in Bytes			
	$\|\mathbb{G}_1\|$	$\|Z_q^*\|$	$\|m\|$	$\|t\|$
Elliptic curve	40	20	20	4
Bilinear pairing curve	128	20	20	4

Table 4.7 shows the communication cost of the proposed SECSP scheme and a comparison of related schemes. From the summary, the overall cost of communication of the study's scheme is given as $4|G_1|+3|Z_q^*| + |t| = 4 \times 40 + 3 \times 20 + 4 = 224\ bytes$. Notably, the proposed scheme surpasses the schemes in (Xiong et al., 2022), (Liu et al., 2020), (Ramadan et al., 2023), and (Zhang et al., 2024) in terms of total communication efficiency. In (Xiong et al., 2022), the total communication cost is given as $7|G_1|+2|Z_q^*| + |t| = 7 \times 128 + 2 \times 20 + 4 = 944\ bytes$. In comparison with the proposed scheme, Xiong et al.'s scheme costs 720 bytes more for single-message communication and 720n bytes more for n messages communication. The total communication cost in (Liu et al., 2020) is given as $6|Z_q^*| + |m| + |t| = 6 \times 768 + 20 + 4 = 792\ bytes$. Comparing this value with the proposed scheme's value, Liu et al.'s scheme costs 568 extra bytes for single message communication and 568n extra bytes for n messages communication. Likewise, in (Ramadan et al., 2023), the total communication cost is given as $4|G_1|+2|m| + |t| = 4 \times 128 + 2 \times 20 + 4 = 556\ bytes$. In comparison with the proposed scheme, Ramadan et al.'s scheme costs 332 bytes more for a single message communication and 332n bytes more for n messages communication. The total communication cost for the scheme in

(Zhang et al., 2024) is computed as $5|G_1|+|\mathrm{Z}_q^*| + |m| + |t| = 5 \times 40 + 20 + 20 + 4 = 244\ bytes$. We note that Zhang et al.'s scheme costs 20 bytes more for single-message communication and 20n bytes more for n messages communication in comparison with the study's scheme. In (Ullah, Alkhalifah, et al., 2021), the total communication cost is given as $2|G_1|+2|\mathrm{Z}_q^*| + |m| + |t| = 2 \times 40 + 2 \times 20 + 20 + 4 = 144\ bytes$. Notably, the total communication cost for Ullah et al.'s scheme is less than the cost of the proposed scheme. Similarly, for the total communication cost in (Zhou, 2019a), we have $4|G_1|+|\mathrm{Z}_q^*| + |t| = 4 \times 40 + 20 + 4 = 184\ bytes$. Notably, Ullah et al.'s scheme and Zhou's scheme slightly outperform the proposed scheme in terms of communication cost, where the proposed scheme costs 80 bytes and 40 bytes more than Ullah et al.'s and Zhou's schemes respectively. However, this is forgivable since the proposed scheme surpasses the schemes in (Ullah, Alkhalifah, et al., 2021) and (Zhou, 2019a) in terms of computation cost. Besides, the overall efficiency (i.e., computational and communication) of the study's scheme is improved against Ullah et al.'s and Zhou's schemes.

The study's scheme improves communication efficiency as follows: In (Xiong et al., 2022), we have; $\frac{944-224}{944} \times 100 = 76.27\%$, in (Liu et al., 2020), we have; $\frac{792-224}{792} \times 100 = 71.72\%$, in (Ramadan et al., 2023), we have; $\frac{556-224}{556} \times 100 = 59.71\%$, while in (Zhang et al., 2024), improvement on communication cost is given as $\frac{244-224}{224} \times 100 = 8.93\%$. The proposed scheme however reduces communication efficiency slightly in comparison with Ullah et al.'s and Zhou's schemes as $\frac{224-144}{224} \times 100 = 35.71\%$ and $\frac{224-184}{224} \times 100 = 17.86\%$, respectively.

Table 4.7

Communication Cost

Scheme	Total communication cost for single message	Total communication cost for *n* messages
(Xiong et al., 2022)	$7\|G_1\|+2\|Z_q^*\| + \|t\| = 944\ bytes$	944n bytes
(Zhou, 2019a)	$4\|G_1\|+\|Z_q^*\| + \|t\| = 184\ bytes$	184n bytes
(Liu et al., 2020)	$6\|Z_q^*\| + \|m\| + \|t\| = 792\ bytes$	792n bytes
(Ullah, Alkhalifah, et al., 2021)	$2\|G_1\|+2\|Z_q^*\| + \|m\| + \|t\| = 144\ bytes$	144n bytes
(Ramadan et al., 2023)	$4\|G_1\| + 2\|m\| + \|t\| = 556\ bytes$	556n bytes
(Zhang et al., 2024)	$5\|G_1\|+\|Z_q^*\| + \|m\| + \|t\| = 244\ bytes$	244n bytes
Proposed	$4\|G_1\|+3\|Z_q^*\| + \|t\| = 224\ bytes$	224n bytes

Table 4.8

Communication Efficiency (%) Improvement of the Proposed Scheme over Related Schemes

Scheme	Efficiency improvement
Xiong et al. 2022	76.27%
Zhou 2019	0.00%
Liu et al. 2020	71.72%
Ullah et al. 2021	0.00%
Ramadan et al. 2023	59.71%
Zhang et al. 2024	8.93%

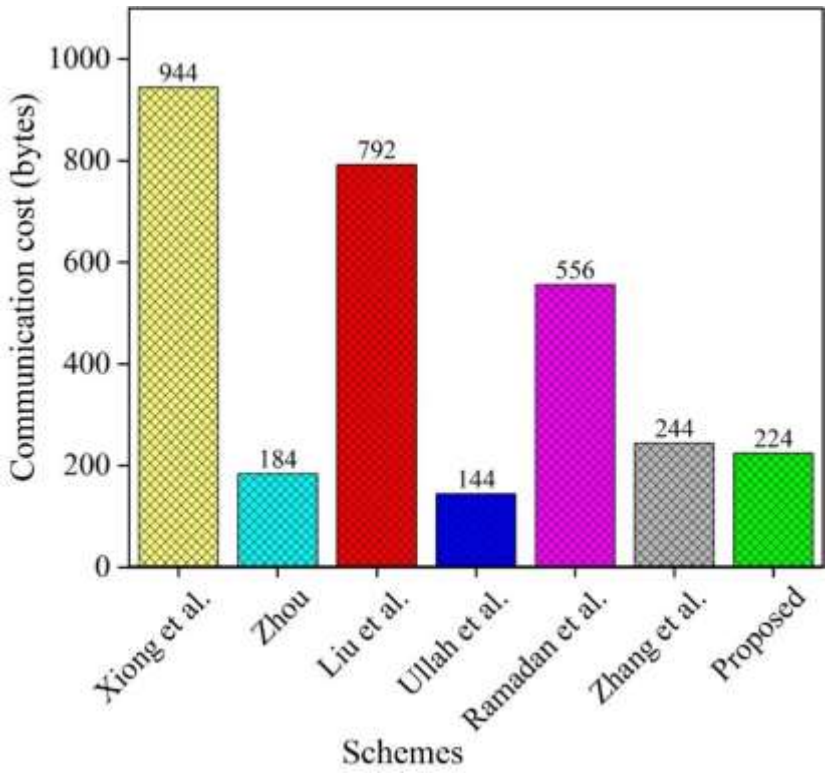

Figure 4.6: Total Communication Cost

4.5. Simulation

This section presents a simulation experiment to evaluate the network performance of the study's scheme. The network metrics considered include throughput, end-to-end delay, and packet loss ratio. In addition, the study compares the results of the proposed scheme with results of schemes in (Xiong et al., 2022), (Zhou, 2019b), (Liu et al., 2020), (Ullah, Alkhalifah, et al., 2021), (Ramadan et al., 2023), and (Zhang et al., 2024).

4.5.1. Simulation Environment and Implementation

The study used Network Simulator 3 (NS-3) as the environment to run simulations, i.e., sending and routing messages from the patient's device to the application provider, while employing the Ad Hoc On-Demand Distance Vector (AODV) as the routing protocol. The simulations were run on a PC whose specifications are as follows: an Intel i7 processor, 8GB of RAM capacity, and a 3.40 GHz CPU. The study conducted a total of 10 simulation experiments for the study's scheme and the schemes in related works, and the average values were obtained for analysis. The parameters and descriptions set in the NS-3 simulator are presented in Table 4.9.

Table 4.9

NS-3 Simulation Parameters

Parameter	Value
Platform	Ubuntu 23.04 LTS
Simulator	NS-3 3.41
Simulation Area	$50m \times 50m$
Simulation Time	120 seconds
Wireless Protocol	IEEE 802.15.6
Wireless Channel Bandwidth	2Mbps
Number of PDs	1,2,3,4,5
Distance between PDs	$10m$
Routing Protocol	AODV

For each network performance metric, the study simulated it as follows: The first experiment involved 1 PD running for 120 seconds and generating values corresponding to the network parameter under investigation. An average value was then computed. The same procedure was then repeated up to 10 times, and the average values recorded in each of the ten experiments were further averaged to obtain a final value. This value corresponds to 1 PD. The same steps were repeated with 2 PDs, 3 PDs, 4 PDs, and 5 PDs.

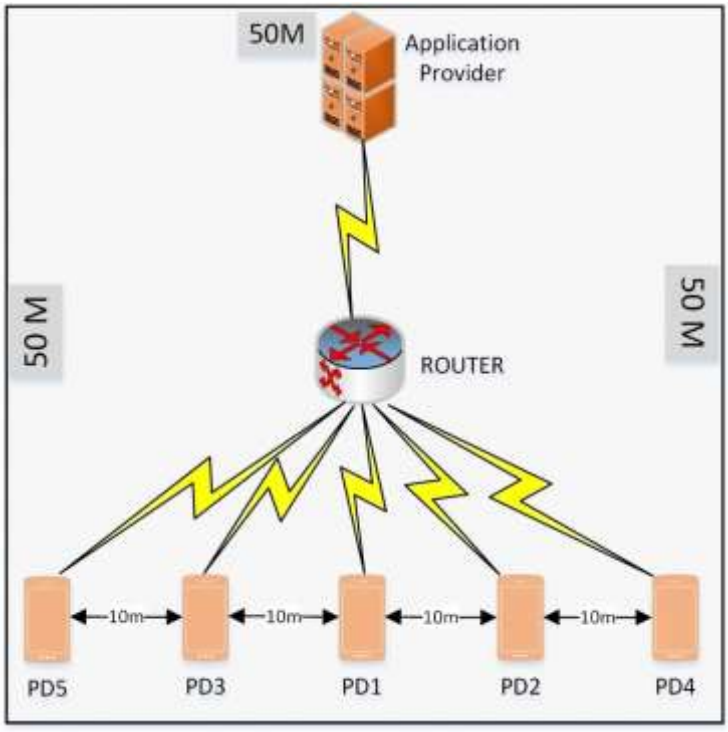

Figure 4.7: Simulation Scenario

Source: Author

4.5.2. Simulation Results

This section presents a discussion of the simulation outcomes for network parameters, including throughput, end-to-end delay, and packet loss ratio.

Throughput

Throughput (T) refers to the total number of messages received by the AP per simulation time, determined using equation 4.1, where M_r and t denote the total messages received and simulation time, respectively.

$$T = \frac{\sum M_r}{\sum t} \tag{4.1}$$

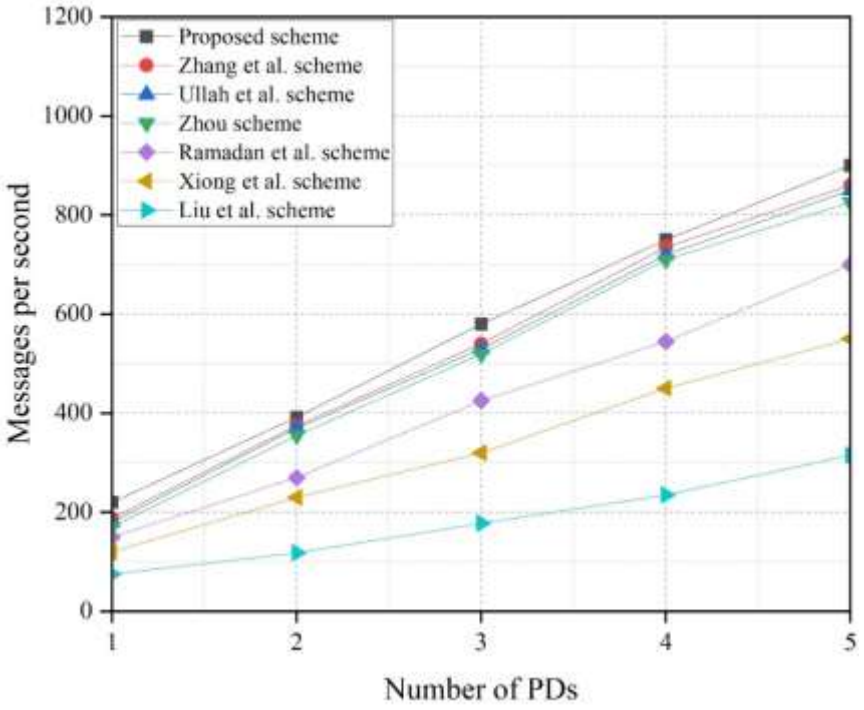

Figure 4.8: Throughput Comparison of Different Schemes

Figure 4.8 demonstrates that throughput increases with an increasing number of PDs for all schemes. This is because as the number of PDs increases, it is obvious that the number of messages transmitted also increases. Notably, the throughput for the proposed scheme is higher than that of other schemes, with the proposed scheme achieving the highest of up to 900 messages when 5 PDs are deployed. On the other hand, with similar number of PDs, schemes in (Xiong et al., 2022), (Zhou, 2019), (Liu et al., 2020), (Ullah et al., 2021), (Ramadan et al., 2023), and (Zhang et al., 2024) have a throughput of 860, 850, 825, 700, 550, and 325 messages, respectively. This is attributed to the higher computational overhead incurred by other schemes, which increases the processing time for messages, thus reducing the number of messages handled per unit time and also introducing additional latency. This renders the proposed scheme more reliable in terms of message throughput.

End-To-End Delay

End-to-end delay (EDD) is measured as the time it takes a message to arrive at the AP from the PD. It can be obtained using equation 4.2, where T_A and T_S denote the time, a message arrived at AP and the time a message was sent from the PD, respectively.

$$EDD = \sum(T_A - T_S) \tag{4.2}$$

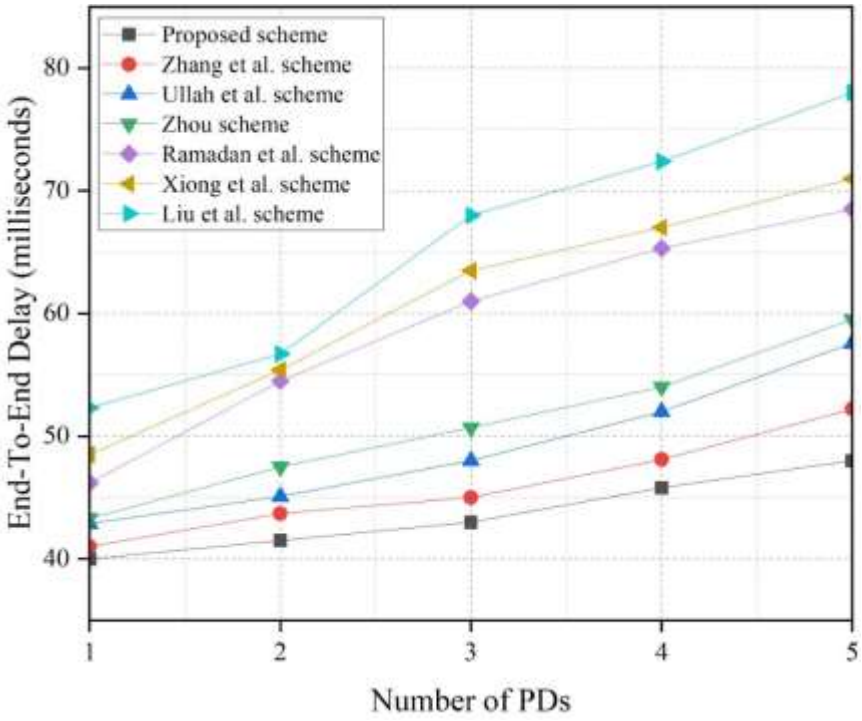

Figure 4.9: End-To-End Delay Comparison of Different Schemes

Adding more PDs corresponds to an increased end-to-end delay in all the schemes, as depicted in figure 4.9. The reason is that as the number of PDs increases, it is expected that the number of messages transmitted over the network too raises, consequently leading to congestion in the network. Congestion results in packets waiting longer in queues, leading to increased delays. However, it is worth noticing that the proposed scheme incurred steady and lowest latency with an average of 43.7 ms compared to schemes in (Xiong et al., 2022), (Zhou, 2019b), (Liu et al., 2020), (Ullah, Alkhalifah, et al., 2021), (Ramadan et al., 2023), and (Zhang et al., 2024) with 46 ms, 49.1 ms, 51 ms, 59.1 ms, 61.1 ms, and 65.5 ms, respectively. Since the proposed scheme outperformed other schemes in terms of computation cost, it is obvious that they incur more processing delays, which accounts for the higher end-to-end delay.

Packet Loss Ratio

As depicted in equation 4.3, packet loss ratio (PLR) is the total number of packets dropped $P_{Dropped}$ divided by the total number of packets sent P_{Sent} by the PD.

$$PLR = \frac{\sum P_{Dropped}}{\sum P_{Sent}} \tag{4.3}$$

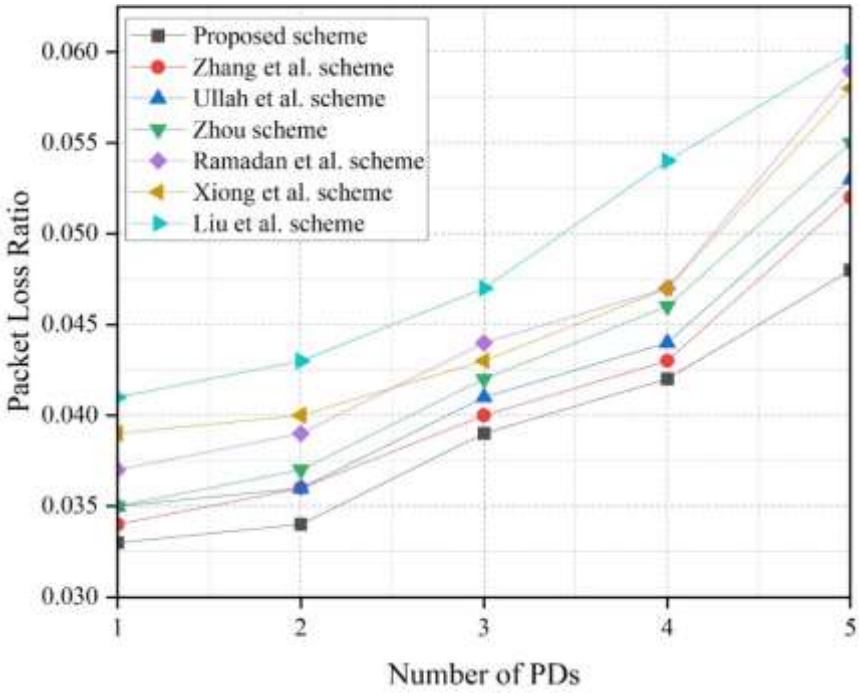

Figure 4.10: Packet Loss Ratio Comparison of Different Schemes

From Figure. 4.10, all the schemes depict a rise in packet loss ratio with an increase in the number of PDs. The increasing density of PDs increases the number of packets generated, and as a result, more message collisions are experienced, leading to increased packet dropping. The proposed scheme indicated a lower packet loss ratio, with an average of 12.4%. Schemes in (Xiong et al., 2022), (Zhou, 2019), (Liu et al., 2020), (Ullah et al., 2021), (Ramadan et al., 2023), and (Zhang et al., 2024) had 17.7%, 23.4%, 27.9%, 28.8%, 29.0%, and 32.7% message dropping, respectively. This is due to the obvious expectation that increased latency experienced by other schemes may cause time-sensitive packets to be dropped if they do not meet the required timing constraints of the network. Additionally, the higher computational cost incurred by other schemes can lead to more processing delays, causing network traffic, which further results in buffer overflows or timeouts. This explains the higher packet loss ratio observed in other schemes.

4.5.3. Discussion

The proposed study's scheme improves the state-of-the-art schemes in terms of the performance metrics evaluated, i.e., security features, computation cost, communication cost and the network performance. This is specifically favourable to WBAN environment which involves resource-constrained devices and high security requirement. For instance,

the use of ECC approach in the study provided a strong security using shorter key length. Similarly, the certificateless nature of the proposed scheme has significantly simplified key management, an operation known to consume a lot of energy. Eventually, this has rendered the proposed scheme more practical in WBAN environment. Likewise, several schemes presented lack security features which the proposed scheme has achieved such as sender authentication e.g., Xiong et al. (2022), conditional anonymity e.g., Zhou (2019a), key escrow resistance, for instance, Ramadan et al. (2023), and forward secrecy, which are critical in WBAN environment. This study therefore has presented an improved model for practical application in the real-world scenario for secure WABN communication. Additionally, the lower communication and computation cost translate to better performance, i.e., in the real-world application, this implies that the WBANs devices' battery life will be prolonged due to reduced energy consumption and the response time for communication being quickened due to the reduced size of data transmitted. While the proposed scheme outperforms the state-of-the-art schemes in terms of the network performance, secure communication, and energy efficiency, further research could focus on constructing schemes which can resist the power of quantum computers by combining the desirable features of ECC and the advanced security features of quantum key distribution (QKD).

CHAPTER FIVE
SUMMARY, CONCLUSION, AND RECOMMENDATIONS

5.1. Summary

The main objective of this research was to design a secure and efficient certificateless signcryption protocol for wireless body area networks using the elliptic curve cryptography and general hash functions to enhance security and efficiency in cryptographic schemes, where resource optimization and data protection is critical. To achieve this objective, the study first conducted an in-depth analysis of the existing WBAN authentication schemes, identifying their strengths and weaknesses in terms of security, computation cost, and communication cost. The review of similar work revealed that existing schemes suffered several weaknesses such as susceptibility to security attacks including the key escrow problem, forgeability, lack of conditional anonymity and forward secrecy, lack of sender authentication among other common attacks. The analysis further shown that many related schemes incurred high computation overhead as well as key management inefficiencies.

Driven by the insights gained from the review of the existing protocols, the study designed a new signcryption protocol that was certificateless in nature to address the limitations identified. The new scheme utilized the elliptic curve cryptography, a technique well known for its desirable features such as strong security with short key sizes, thus significantly improving on security and efficiency of communication in resource-constrained environments like WBANs. The design focused on enhancing security features not addressed in other related schemes such as ensuring data confidentiality, unforgeability, key escrow resistance, sender authentication, forward secrecy, conditional anonymity, and typical WBAN attacks. Finally, the design focused on optimizing computational and communication efficiency as well as network performance.

To validate the suitability of the proposed scheme in WBAN environment, the study further conducted performance evaluation in terms of security features, computation cost, communication cost, and network performance. To evaluate security, the study conducted both formal and informal security analysis. The formal security analysis involved carrying out security prove using the Random Oracle Model (ROM) to prove the schemes confidentiality and unforgeability features. The results of the proof revealed that the

proposed scheme is indistinguishable against chosen ciphertext attack (IND-CCA) and existentially unforgeable against adaptively chosen-message attacks (EUF-CMA). Informal analysis entailed the analysis of other security features necessary for WBAN communication, where the proposed scheme proved to meet all the features considered in the evaluation. Performance evaluation in terms of communication and computation cost revealed a significant improvement in efficiency, where the proposed scheme improves the existing schemes' efficiency by over 50%. Besides, the network performance evaluation conducted through simulation to determine the scheme's performance in terms of throughput, end-to-end delay, and packet loss ratio revealed that the proposed scheme outsmarts the state-of-the art schemes.

5.2. Conclusion

This study has successfully achieved its objective by analyzing, designing and validating secure and efficient certificateless signcryption for wireless body area networks by utilizing elliptic curve cryptography (ECC). The analysis of existing protocols provided some insights on existing limitations on security, communication cost and computational cost. Building on the findings from the analysis, the study designed a new secure and efficient signcryption protocol based using the elliptic curve cryptography and general hash functions to address the weaknesses found in the existing schemes. The design achieved significant improvement in terms of performance through optimizing the cost for computational algorithms and that of communication, thus making it suitable for resource constrained WBAN devices. Through comprehensive performance evaluation, the results proved the scheme to outsmart the state-of-the art schemes across the key performance metrics i.e., security, computation cost, communication cost, and network performance. This validation confirms that the proposed scheme is not only secure but also efficient in terms of resource usage, thereby enhancing WBAN reliability and usability for healthcare applications.

5.3. Recommendations

Firstly, the study recommends the adoption of the proposed secure and efficient certificateless signcryption protocol for resource-constrained environments such as WBANs. Secondly, focusing on certificateless cryptography, researchers and developers

should carry out continuous security audits of the existing and emerging schemes to identify vulnerabilities, especially as new attack vectors and threats evolve. Lastly, future research should conduct real-world testing in actual WBAN environment to gain full understanding of scheme's performance under real-world conditions. Broader range of attack scenarios should be considered during validation to ensure the robustness of the protocol in a wider array of potential threats.

5.4. Suggestion for Further Research

Based on the idea of hard problems that can't be solved by computers, this study created a signcryption protocol to keep messages safe using elliptic curve cryptography. However, with the emerging power of quantum computing, this assumption may not apply. In the future, this study intends to improve the proposed scheme by exploring and developing a hybrid cryptographic framework that combines the strengths of ECC with the advanced security features of quantum key distribution (QKD) to create a robust and future-proof cryptographic system that can withstand the capabilities of quantum computers while maintaining the practical benefits of ECC.

REFERENCES

Abiramy, N. V, Smilarubavathy, G., Nidhya, R., & Kumar, D. A. (2018). A secure and energy efficient resource allocation scheme for wireless body area network. *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference On*, 729–732.

Al-Riyami, S. S., & Paterson, K. G. (2003). Certificateless public key cryptography. *International Conference on the Theory and Application of Cryptology and Information Security*, 452–473.

Al Barazanchi, I., Hashim, W., Alkahtani, A. A., Abbas, H. H., & Abdulshaheed, H. R. (2021). Overview of WBAN from literature survey to application implementation. *2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 16–21.

Ali, I., Chen, Y., Ullah, N., Kumar, R., & He, W. (2021). An Efficient and Provably Secure ECC-Based Conditional Privacy-Preserving Authentication for Vehicle-to-Vehicle Communication in VANETs. *IEEE Transactions on Vehicular Technology*, *70*(2), 1278–1291.

Almuhaideb, A. M. (2022). Secure and Efficient WBAN Authentication Protocols for Intra-BAN Tier. *J. Sens. Actuator Netw*, *11*(44).

Asam, M., Jamal, T., & Ajaz, A. (2019). Challenges in Wireless Body Area Network. *International Journal of Advanced Computer Science and Applications*, *10*(11), 336–341.

Bellare, M., & Rogaway, P. (1996). The exact security of digital signatures-How to sign with RSA and Rabin. *International Conference on the Theory and Applications of Cryptographic Techniques*, 399–416.

Cornet, B., Fang, H., Ngo, H., Boyer, E. W., & Wang, H. (2022). An Overview of Wireless Body Area Networks for Mobile Health Applications. *IEEE Network*, *36*(1), 76–82.

Dai, S., Jiang, L., He, S., & Guo, D. (2018). An energy efficient authentication scheme for

wireless body area networks based on the bilinear pairings. *International Journal of Internet Protocol Technology*, *11*(4), 232–241.

Deng, Y. X., & Shi, R. H. (2018). An efficient remote anonymous authentication scheme with user revocation. *International Journal of Security and Networks*, *13*(2), 84–97.

Diffie, W., & H. (1976). New directions in croptography. *IEEE Transactions on Information Theory*, *22*(6), 159.

Fotouhi, M., Bayat, M., Das, A. K., Far, H. A. N., Pournaghi, S. M., & Doostari, M. A. (2020). A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Computer Networks*, *177*(May).

Hasan, K., Ahmed, K., Biswas, K., Islam, M. S., Kayes, A. S. M., & Islam, S. M. R. (2020). Control plane optimisation for an SDN-based WBAN framework to support healthcare applications. *Sensors*, *20*(15), 4200.

Jahan, M., Zohra, F. T., Parvez, K., Kabir, U., Mohaimen, A., Radi, A., & Kabir, S. (2018). An End-to-End Authentication Mechanism for Wireless Body Area Networks. *ArXiv Preprint ArXiv*, *2111*(06158).

Jegadeesan, S., Azees, M., & Babu, N. R. (2020). EPAW : Efficient Privacy Preserving Anonymous Mutual Authentication Scheme for Wireless Body Area Networks (WBANs). *IEEE Access*, *8*, 48576–48586.

Ji, S. A. I., Gui, Z., & Zhou, T. (2018). An Efficient and Certificateless Conditional Privacy-Preserving Authentication Scheme for Wireless Body Area Networks Big Data Services. *IEEE Access*, *6*, 69603–69611.

Kasyoka, P. N. (2022). *Certificateless Signcryption for Wireless Sensor Networks*.

Kim, B.-S., Sung, T.-E., & Kim, K.-I. (2020). An ns-3 implementation and experimental performance analysis of ieee 802.15. 6 standard under different deployment scenarios. *International Journal of Environmental Research and Public Health*, *17*(11), 4007.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, *48*(177), 203–209.

Kompara, M., Islam, S. H., & Hölbl, M. (2019). A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs. *Computer Networks*, *148*, 196–213.

Konan, M., & Wang, W. (2019). A secure mutual batch authentication scheme for patient data privacy preserving in WBAN. *Sensors (Switzerland)*, *19*(7).

Koya, A. M., & P. P., D. (2018). Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network. *Computer Networks*, *140*, 138–151.

Kumar, M., & Hussain, S. Z. (2023). An efficient and secure mutual authentication protocol in wireless body area network. *EAI Endorsed Transactions on Pervasive Health and Technology*, *9*.

Li, A. A. O. (2018). Provably Secure Heterogeneous Access Control Scheme for Wireless Body Area Network. *J Med Syst*, *42*(108), 190–198.

Li, F. (2018). Cost-Effective and Anonymous Access Control for Wireless Body Area Networks. *IEEE Systems Journal*, *12*(1), 747–758.

Li, X., Ibrahim, M. H., Kumari, S., Sangaiah, A. K., Gupta, V., & Choo, K. K. R. (2017). Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. *Computer Networks*, *129*, 429–443.

Liu, X., Wang, Z., Ye, Y., & Li, F. (2020). An efficient and practical certificateless signcryption scheme for wireless body area networks. *Computer Communications*, *162*(February), 169–178.

Mandal, S. (2022). Provably secure certificateless protocol for wireless body area network. *Wireless Networks*, *4*.

Meng, X. (2019). *An Anonymous Mutual Authentication and Key Agreement Scheme in WBAN*. 31–36.

Miller, V. S. (1985). Use of elliptic curves in cryptography. *Conference on the Theory and Application of Cryptographic Techniques*, 417–426.

Noor, F., Kordy, T. A., Alkhodre, A. B., Benrhouma, O., Nadeem, A., & Alzahrani, A. (2021). Securing Wireless Body Area Network with Efficient Secure Channel Free and Anonymous Certificateless Signcryption. *Wireless Communications and Mobile Computing*, *2021*.

Omala, A. A., Ali, I., & Li, F. (2018). Heterogeneous signcryption with keyword search for wireless body area network. *Security and Privacy*, *1*(5), e25.

Qu, Y., Zheng, G., Ma, H., Wang, X., Ji, B., & Wu, H. (2019). A survey of routing protocols in WBAN for healthcare applications. *Sensors (Switzerland)*, *19*(7).

Ramadan, M., Raza, S., & Member, S. (2023). Identity-Based Signcryption for Telemedicine Systems. *IEEE Internet of Things Journal*, *10*(18), 16594–16604.

Rehman, Z. I. A. U. R., Altaf, S., Ahmad, S., Al-shayea, A. M., & Iqbal, S. (2021). An Efficient , Hybrid Authentication Using ECG and Lightweight Cryptographic Scheme for WBAN. *IEEE Access*, *9*, 133809–133819.

Safa, N. S., Maple, C., Haghparast, M., Watson, T., & Dianati, M. (2019). An opportunistic resource management model to overcome resource-constraint in the Internet of Things. *Concurrency and Computation: Practice and Experience*, *31*(8), e5014.

Shamir, A. (1984). Identity-Based Cryptosystems and Signature Schemes. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *196 LNCS*, 47–53.

Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., & Tang, Y. (2018). Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *Journal of Network and Computer Applications*, *106*, 117–123.

Shuai, M., Liu, B., Yu, N., Xiong, L., & Wang, C. (2020). Efficient and privacy-preserving authentication scheme for wireless body area networks. *Journal of Information Security and Applications*, *52*.

Tchórzewski, J., & Jakóbik, A. (2019). Theoretical and experimental analysis of cryptographic hash functions. *Journal of Telecommunications and Information Technology*, *1*, 125–133.

Teshome, A. K., Kibret, B., & Lai, D. T. H. (2018). A Review of Implant Communication Technology in WBAN: Progress and Challenges. *IEEE Reviews in Biomedical Engineering*, *12*(c), 88–99.

Ullah, I., Alkhalifah, A., Rehman, S. U., Kumar, N., & Khan, M. A. (2021). An Anonymous Certificateless Signcryption Scheme for Internet of Health Things. *IEEE Access*, *9*, 101207–101216.

Ullah, I., Zeadally, S., Amin, N. U., Khan, M. A., & Khattak, H. (2021). Lightweight and provable secure cross-domain access control scheme for internet of things (IoT) based wireless body area networks (WBAN). *Microprocessors and Microsystems*, *81*, 103477.

Umar, M., Wu, Z., Liao, X., Chen, J., & Muhammad, B. A. (2021). Efficient Anonymous Authentication Scheme in Body Area Networks Via Signal Propagation Characterization. *Journal of Networking and Network Applications*, *1*(2), 49–59.

Vyas, A., & Pal, S. (2020). Preventing security and privacy attacks in WBANs. *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 201–225.

Wu, X., Xu, J., Huang, W., & Jian, W. (2020). *A new mutual authentication and key agreement protocol in wireless body area network*. 199–203.

Xie, Y., Zhang, S., Li, X., Li, Y., Chai, Y., & Zhang, M. (2019). CasCP: Efficient and Secure Certificateless Authentication Scheme for Wireless Body Area Networks with Conditional Privacy-Preserving. *Security and Communication Networks*, *2019*.

Xiong, H., Hou, Y., Huang, X., Zhao, Y., & Chen, C. M. (2022). Heterogeneous Signcryption Scheme From IBC to PKI With Equality Test for WBANs. *IEEE Systems Journal*, *16*(2), 2391–2400.

Xu, J., Meng, X., Liang, W., Zhou, H., & Li, K.-C. (2020). A secure mutual authentication scheme of blockchain-based in WBANs. *China Communications*, *17*(9), 34–49.

Yang, X., Yi, X., Khalil, I., Huang, X., & Shen, J. (2022). Efficient and Anonymous Authentication for Healthcare Service With Cloud Based WBANs. *IEEE Transactions on Services Computing*, *15*(5), 2728–2741.

Yao, M., Wang, X., Gan, Q., Lin, Y., & Huang, C. (2021). An Improved and Privacy-Preserving Mutual Authentication Scheme with Forward Secrecy in VANETs. *Security and Communication Networks*, *2021*.

Zhang, J., Dong, C., & Liu, Y. (2024). Efficient Pairing-Free Certificateless Signcryption Scheme for Secure Data Transmission in IoMT. *IEEE Internet of Things Journal*, *11*(3), 4348–4361.

Zhang, J., Zhang, Q., Li, Z., Lu, X., & Gan, Y. (2021). A Lightweight and Secure Anonymous User Authentication Protocol for Wireless Body Area Networks. *Security and Communication Networks*, *2021*.

Zheng, Y. (1997). Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption). *Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings 17*, 165–179.

Zhou, C. (2019a). An improved lightweight certificateless generalized signcryption scheme for mobile-health system. *International Journal of Distributed Sensor Networks*, *15*(1), 1550147718824465.

Zhou, C. (2019b). *An improved lightweight certificateless generalized signcryption scheme for mobile-health system*. *15*(1).

APPENDICES

Appendix I: Tharaka University Introductory Letter

THARAKA UNIVERSITY

P.O BOX 193-60215,
MARIMANTI, KENYA

Telephone: +(254)-0202008549
Website: https://tharaka.ac.ke
Social Media: tharakauni
Email: info@tharaka.ac.ke

OFFICE OF THE DIRECTOR
BOARD OF POSTGRADUATE STUDIES

REF: TUN/BPGS/PL/03/24 — **12th March, 2024**

To Whom It May Concern

Dear Sir/Madam,

RE: MISHECK MURIMI KING'ANG'I ADMISSION NUMBER SMT22/03130/20

Mr. Misheck Murimi King'ang'i is a postgraduate student at Tharaka University undertaking a Master degree in **Computer Science**. The student has completed his coursework and is expected to proceed for collection of data after successfully defending his proposal at faculty level. The title of the study is "***Secure and Efficient Certificateless Signcryption Protocol for Wireless Body Area Networks.***" The proposed study will be carried out in **Tharaka University.**

Any assistance accorded to him will be highly appreciated.

Thank you in advance.

Yours faithfully,

THARAKA UNIVERSITY
12 MAR 2024
DIRECTOR
P.O. BOX 60215, MARIMANTI

Dr. Marciano Mutiga, PhD
Director, Board of Postgraduate Studies.

Appendix II: Institutional Ethics Review Letter

THARAKA UNIVERSITY

P.O BOX 193-60215,
MARIMANTI, KENYA

Telephone: +(254)-0202008549
Website: https://tharaka.ac.ke
Social Media: tharakauni
Email: info@tharaka.ac.ke

INSTITUTIONAL SCIENTIFIC AND ETHICS REVIEW COMMITTEE

20th February, 2024.

REF: TUNISERC/NSEC/M009

Dear, Misheck Murimi Kingangi

RE: Secure and Efficient Certificateless Signcryption Protocol for Wireless Body Area Networks

This is to inform you that ***Tharaka University ISERC*** has reviewed and approved your above research proposal. Your application approval number is ***ISERC04023.*** The approval period is ***20th February 2024 –20th February, 2025.***

This approval is subject to compliance with the following requirements;

i. Only approved documents including (informed consents, study instruments, MTA) will be used
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by ***Tharaka University ISERC***.
iii. Death and life threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to ***Tharaka University ISERC*** within 72 hours of notification
iv. Any changes, anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to ***Tharaka University ISERC*** within 72 hours
v. Clearance for export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days upon completion of the study to ***Tharaka University ISERC***.

Prior to commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology and Innovation (NACOSTI) https://research-portal.nacosti.go.ke and also obtain other clearances needed.

Yours sincerely,

Dr. Fidelis Ngugi
Chair, ISERC Tharaka University

Appendix III: NACOSTI License

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **815572**

Date of Issue: **17/April/2024**

RESEARCH LICENSE

This is to Certify that Mr.. Misheck Murimi King'ang'i of Tharaka University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Tharaka-Nithi on the topic: Secure and Efficient Certificateless Signcryption Protocol for Wireless Body Area Networks for the period ending : 17/April/2025.

License No: **NACOSTI/P/24/34278**

815572

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions