CERTIFICATELESS SIGNCRYPTION FOR WIRELESS SENSOR NETWORKS

PHILEMON NTHENGE KASYOKA

DOCTOR OF PHILOSOPHY

(Computer Science)

JOMO KENYATTA UNIVERSITY OF

AGRICULTURE AND TECHNOLOGY

2022

Certificateless Signcryption for Wireless Sensor Networks

Philemon Nthenge Kasyoka

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Philosophy in Computer Science of the Jomo Kenyatta University of Agriculture and Technology

2022

DECLARATION

This thesis is my original work and has not been presented for a degree in any other University.

Signature …………………………………….. Date……………………..

Philemon Nthenge Kasyoka

This Thesis has been submitted for examination with our approval as the University supervisors:

Signature…………………………………… Date………………………..

Dr. Michael Kimwele, PhD

JKUAT, Kenya

Signature……………………………………. Date………………………

Dr. Shem Mbandu Angolo, PhD

Co-operative University of Kenya

DEDICATION

This research study is dedicated to my mother Rosemary, my wife Pendo, my sons Zion and Shiloh and my daughter Zoe.

ACKNOWLEDGEMENTS

I would like to thank God the almighty for blessing me with opportunity and the provisions required all through my Doctorial studies. I express my deepest gratitude to my two supervisors: Dr. Michael Kimwele and Dr. Shem Mbandu Angolo who patiently guided me through my entire research work. It has been a great pleasure to write this thesis under their guidance, insightful comments and encouragement. I am also grateful to my dear wife Pendo, my sons Zion and Shiloh and daughter Zoe for their encouragement and support during my Doctorial studies. Lastly, I would like to thank Jomo Kenyatta University of Agriculture and Technology for providing such a great academic environment and resources that made my Doctorial studies rewarding and memorable.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

APPENDICES

ABBREVIATIONS AND ACRONYMS

BDHP	Bilinear Diffie-Hellman Problem
CCA	Chosen Ciphertext Attack
CBDHP	Computational Bilinear Diffie-Hellman Problem
CDHP	Computational Diffie-Hellman Problem
CLC	Certificateless Cryptography
CLSC	Certificateless Signcryption
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDHP	Elliptic Curve Diffie-Hellman Problem
EUF-CMA	Existential Unforgeability under Chosen Message Attack
IBE	Identity Based Encryption
PKI	Public Key Infrastructure
PKG	Public Key Generator
PPT	Probabilistic Polynomial Time
KGC	Key Generation Center
ROM	Random Oracle Model
WSN	Wireless Sensor Network
WBAN	Wireless Body Area Network

ABSTRACT

Wireless sensor networks (WSNs) have become popular in the field of information and communications technology, they are increasingly being used in applications such as surveillance systems, patient monitoring, object tracking, forest fire detection and habitat monitoring among others. By its very nature, a WSN provides a resource constrained environment where devices used are limited in resource usage. Due to these limitations, security challenges have emerged in their applications. Hence, the need for computationally efficient but still secure cryptosystems. Traditional cryptographic primitives cannot be directly applied on WSNs due to their resource constrained nature, this has led to the challenge of achieving cryptographic security goals which are important for effective communication of information on WSNs. Recent studies have shown that it is possible to apply public key cryptography such as ECC to resource constrained devices by using the right selection of algorithms and associated parameters, optimization and low power concepts. To address security challenges on WSNs, this thesis proposed an efficient digital signature scheme, a variant of ECDSA that can be applied on WSNs to provide authentication. Further, the variant of ECDSA was used in the design of a signcryption schemes. The signcryption schemes are intended to be efficient enough for use on WSNs and for that reason the research work focused on certificateless cryptography (CLC) for the design of the signcryption scheme with a property of ciphertext authenticity. The research methodology employed was experimental. Major contributions of this research were an efficient variant of ECDSA more efficient in the signing and verification process that does not suffer from the security challenges inherent in the original ECDSA. Out of the proposed digital signature scheme a certificateless pairing free authentication scheme for wireless body area network in healthcare management system and a multi-user broadcast authentication scheme for WSNs were constructed. Three certificateless signcryption schemes were designed, two signcryption schemes were designed from the proposed ECDSA variant and one signcryption was a modification of a scheme by Wei and Ma (2019). A formal security proof for indistinguishability against adaptive chosen ciphertext attack and existential unforgeability against adaptive chosen message attack was provided for the three signcryption schemes in the random oracle model. The signcryption schemes were more efficient with respect to computational cost, communication overhead and energy consumption comparison with other existing related schemes.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Wireless Sensor Networks (WSNs) over the years are increasingly gaining popular due to rapid technological advancements in wireless communication technologies. They have potential applications in different area including environment, health and military (Bensaleh et al., 2020). A Wireless Sensor Network is a type of wireless ad hoc network that runs autonomously and has the capability to deploy a large number of low-cost sensor devices distributed over a selected area of interest. These sensors can sense and monitor the physical phenomenon in a given environment and transmit information collected to a base station. The base station coordinates the operations of the entire sensor networks, makes decisions, assigns various tasks and has the ability to make query and retrieve requested data from the network. The sensors are also referred to as nodes and are resource constrained in nature (Kardi et al., 2018). They have low communication bandwidth, computation, power consumption and storage capacity and as a result they pose a challenge in the application of traditional cryptographic security protocols/schemes in the WSN.

Wireless Sensor Network's security is becoming a challenge because of the openness and resource constrained nature of its network architecture, without an effective security mechanism an attacker can capture information from its nodes and can use it for malicious purposes. There is an urgent need to ensure all basic security goals such as confidentiality, integrity, unforgeability, non-repudiation, forward secrecy and public verifiability are achieved in a more efficient manner in resource constrained environments (Patil et al., 2016; Singh & Vaisla, 2014). A lot of research efforts have been devoted to address security WSNs (Ullah et al., 2021; Fang et al., 2019; Omala et al., 2018; Wahid & Mambo, 2016; Won et al., 2015).

A security protocol is expected to make use of security mechanisms consisting of cryptographic primitives such as encryption or a digest for message authentication and integrity. Traditional primitives form the basis of security protocols. However, they consume a fair amount of energy during computation. Since Elliptic Curve Cryptography (ECC) was invented by (Miller, 1985) and (Kobiltz, 1987), it has gained increasing popularity as a building block of public key cryptography due to its ability to generate small and efficient keys. Using ECC presents a great advantage in a few unique areas. For instance, elliptic curve-based systems require less memory compared to RSA based schemes. A key size of 4096 bits in RSA will give the same level of security as 313 bits in an elliptic curve system and this presents us with an opportunity to use ECC for development of cryptographic schemes for use on resource limited devices.

With the need to ensure all security goals are achieved signatures and encryption techniques were used and this led to the concept of signcryption proposed by (Zheng, 1997). Signcryption is cryptographic primitive that simultaneously provide both the function of digital signature and public key encryption in a single logical step (Gao et al., 2019). The computation and communication cost of signcryption scheme is more efficient than schemes based on sign-then-encrypt concept (Ashraf et al., 2014) and for that reason signcryption can be very useful in areas such as Wireless Sensor Networks, mobile ad hoc networks among other areas (Chaitra & RaviKumar, 2021; Mandal et al., 2016).

In conventional signcryption users choose their own private keys, compute corresponding public keys and submit them to a certificate authority for issuance of certificates. This approach creates a need for infrastructure known as Public Key Infrastructure (PKI). The PKI deals with the issues associated with certificate management, including revocation, storage, distribution and the computational costs of certificate verification.

In 1984, (Shamir, 1984) introduced the notion of ID-Based cryptography to mitigate the need for PKI. Identity Based Encryption (IBE) provides a public key encryption mechanism a string such as an email address (e.g., kasyoka@jkuat.ac.ke) can be used as a public key eliminating the need of public key certification such as PKI (Lee et al., 2020). In an IBE system, users authenticate themselves to the PKG and obtain private keys corresponding to their identities; this leads to the need to establish a key escrow mechanism which is a major drawback in terms of security and efficiency (Boneh & Franklin, 2003).

In 2003, (Al-Riyami & Paterson, 2003) introduced the concept of certificateless cryptosystem to address the issue of key escrow while still avoiding use of certificates. The approach involves partitioning of a private key into two parts. In the first part Key Generating Center (KGC) generates partial private key d and send to a user through a secure channel. The second part involves the user generating a secret key x making the full private key fk to be $fk = (d, x)$. The secret key x is unknown to the KGC (Boneh & Franklin, 2003). Traditional cryptographic primitives are not able to achieve lightweight signcryption schemes for use on resource constrained devices due to high computation power requirement, more communication overhead incurred and large memory requirements.

With the ECC proven to offer more efficient schemes (Sarath et al., 2014) compared to other primitives such as RSA in terms of key-size, this provides an opportunity for development of lightweight cryptographic schemes for use on resource constrained devices.

1.2 Problem Statement

Security issues in WSNs are increasingly receiving a lot of attention from many researchers due to the dependency of many critical human and environmental applications on such networks and there is an essential need to ensure total security of data collected and transmitted through such networks. Most of the security goals in WSNs can be achieved through digital signatures and encryption. However, traditional cryptographic primitives cannot be directly applied in such networks due to their resource constrained nature and this makes them more vulnerable to security attacks (Zang et al., 2022). Conventional public key encryption algorithms require intensive computations and are considered inefficient for use on WSNs (Kardi et al., 2018; Al-Shehri, 2017) hence the continuing need for more lightweight cryptographic primitives that will be more efficient in computation, communication overhead and reduce the amount of energy cost.

ECC has become popular due to its acceptance as an efficient cryptographic primitive hence a good candidate for design of security scheme for resource constrained environments. ECDSA uses two modular multiplicative inverse operations which are time-consuming and the verification process of ECDSA is slow (Genc and Afacan., 2021). Considering the fact that in most applications of digital signatures, signers are more than verifier, the need to speed up EC primitives for use on resource constraints devices is a problem of considerable practical importance. The concept of signcryption has been proven to be more efficient than sign-then-encrypt approach (Ullah et al., 2021) and this has led to the concept of signcryption.

A signcryption scheme that avoids use of PKI can be useful in WSNs since sensor nodes in WSNs are resource constrained in nature. ID-based schemes do not use PKI however they make use of key escrow which presents a security challenge and for that reason the focus of this research is on certificateless cryptography. Several certificateless signcryption schemes exist. However, most of the signcryption schemes proposed have complex computations or do not address all basic security goals applicable to WSNs such as confidentiality, integrity, public verifiability, unforgeability, forward secrecy, data freshness and ciphertext authenticity (Costa et al., 2017; Li et al., 2018). This thesis has proposed a more efficient digital signature scheme and applied it in the design of more efficient certificateless signcryption schemes for use on Wireless Sensor Networks that are secure in the aforementioned security goals.

1.3 Justification

WSNs networks are by nature resource constrained as they are composed of devices that are limited in terms of storage, computation and even power consumption. They are used in many different applications WSNs can be applied in monitoring for potential enemy intrusion. When an intrusion is detected by a sensor, a warning message will be used to report the event through possibly multi-hop communications to a remote base station for appropriate actions to be taken. In such a setting, to securely send a warning from a node sensing an intrusion, all communicating nodes should be able to authenticate each other, make sure that the report is not from an intruder and the report transmitted should not be detected by an intruder. A security scheme should be in place to resist various serious attacks such as Sybil, node duplication, wormhole, and bogus message injection attacks. There are many separate solutions to addressing the aforementioned issues however; it is difficult to combine them due to different or conflicting underlying assumptions. Even if it is possible to combine these solutions, it is far too complex to implement such a solution on a resource constrained environment such as one provided by a Wireless Sensor Networks.

Traditional security mechanisms are complex and require a lot of resources and for that reason they cannot be directly applied on WSNs nodes hence need for more efficient security scheme (Xu et al., 2015; Alrehily et al., 2015), there inefficiency inhibits wide spread adoption within the ultra-low energy regimes such as WSNs, Smart cards and Radio Frequency Identification tags (RFIDs).

In some critical application areas such as ubiquitous healthcare WSNs devices are required to be available all through especially where they are used to control critical tasks such as administration of drugs or monitor patients vital signs, however lack of proper security may make them susceptible to attacks such as Denial-of-Service attack forcing them to shut down and this can lead to loss of life, hence the urgent need to ensure effective lightweight cryptographic schemes for such constrained environments are designed and adopted (Al-Shehri, 2017). ECC is a promising approach since it significantly reduces the key sizes and hence is more relevant in the context of WSNs than other asymmetric primitives such as RSA. A certificate is used to bind each user public key and its corresponding user identity. Management of certificates in public key infrastructure is a complex task that makes PKI systems not suitable for use in WSNs while the IBC make use of key escrow which has substantial vulnerabilities. With regard to the current technological advancements there is a compelling need for an efficient and highly secure cryptographic scheme that can meet the requirements of resource-constrained devices (Ullah et al., 2019). This research work intents to focus on certificateless cryptography which is more efficient since it does not require certificate management and does not use key escrow.

1.4 General Objective

The general purpose of this research is to develop a signcryption scheme that seeks to ensure efficient and secure communication in resource constrained environments such as Wireless Sensor Networks.

1.5 Specific Objectives

i. To investigate the techniques that can be used to adopt traditional digital signature primitives for use on Wireless Sensor Networks.
ii. To design an efficient digital signature scheme, a variant of the ECDSA suitable for Wireless Sensor Networks.
iii. To use the proposed signature scheme in the design of a secure and lightweight certificateless signcryption scheme.
iv. To test the efficiency and security of the proposed schemes.

1.6 Research Questions

i. What are the techniques that can be used to adopt traditional digital signatures schemes for use on Wireless Sensor Networks?
ii. How will an efficient Digital signature scheme suitable for Wireless Sensor Networks be designed?
iii. How will the proposed digital signature be used in the design of a secure and lightweight certificateless signcryption scheme?
iv. How will the proposed schemes be tested for security and efficiency?

1.7 Scope

This research work covered digital signatures from the perspective of Elliptic Curve cryptographic as well as pairing-free certificateless signcryption scheme based on Elliptic Curves. Further, an application area for each of the cryptographic protocols is provided.

CHAPTER TWO

LITERATURE REVIEW

2.1 Resource Constrained Devices

The resource constrained devices are devices that are limited in computation power, memory or storage capacity and have a low power capacity (Safa et al., 2019). Their inefficiency prevents wide spread adoption within environments such as Wireless Sensor Networks, Implantable Medical Devices, Smart cards and IoT among others. IoT devices often operate on lossy and low-bandwidth communication channels. As IoT devices become more integrated with our society (eg, smart city, smart home) there is need to understand, manage and mitigate security risks involved (Choo et al.,2020). However, It seems to be impossible to directly apply standard conventional security protocols of the Internet in the context of IoT.

Mobile devices and other hand-held devices are compact and lightweight and fall under the category of resource constrained devices. Technological advancement in data storage, display and design have allowed these hand-held devices to do nearly anything that had previously been reserved for larger personal computers. RFID is an innovative technology that provides us with the ability to gather amounts of data that is related to products, assemblies, supplies, inventory, customer service, and machinery. With the increasing popularity of RFID tags, data privacy is becoming a major concern. Anyone can track tags and find the identity of any objects fitted with the tags. As technological advancements in wearable technology continue to gather pace, an opportunity to connect our bodies to the Internet through tiny sensor nodes implanted in our bodies becomes obvious. However, this can easily lead to theft of our physiological data (Nguyen et al., 2015).

These devices have become more prevalent in daily life. Although improvements in hardware and software have enabled more complex tasks to be performed on such devices, this functionality has also increased the attractiveness of the platform as a target for attackers, hence the need for a computationally cheap, but still secure, cryptosystem rises. The most serious restrictions of resource constrained devices can be narrowed to two categories: computational limitations and power limitations. They are used to process, store and communicate information in areas such as Wireless Sensor Networks, Wireless Body Area Networks, e-commerce, Internet-of-Things (IoT), RFID, medical healthcare among other areas.

Smart cards such as SIM cards have been proposed for applications like secure access to services in GSM, to authenticate users and secure payment using Visa cards and MasterCard. Wireless transactions are facing several security challenges. Data sent through air face almost the same security threats as the data over wired networks and even more (Elkamchouchi et al., 2014). The fact that RC devices are resource limited presents a lot of challenges when providing security to data processed, stored and transmitted using such devices.

Most security protocols implemented on wired-line networks have been adopted for use in wireless networks. However, they have been found not to be suitable for wireless networks and devices since scenarios and capabilities applicable to wired-line networks may not be valid in wireless networks. It may be possible to perform several complex computations on a typical wired network. However, such computations may deplete battery power on devices running due to limited battery power.

on wireless network. Cryptographic primitives can consume a fair amount of energy that can degrade the battery performance of wireless network. Since the traditional cryptographic primitives would be resource draining in such environments and could introduce unnecessary delays in processing hence the need for more optimized security primitives. In order to guarantee the security in resource constrained devices, research on robust lightweight security solutions are of practical importance.

Lightweight cryptographic primitives are important and they consist of cryptographic algorithms that meet the requirement of constrained environments. It is worth noting that, this does not suggest they are any less secure. They provide a low power computation and low energy consumption ciphers. In addition, they support a sufficient security level even if adapted to resource-limited devices.

2.2 Wireless Sensor Networks

Wireless sensor network has the capacity to configure itself, an infrastructure less wireless network consisting of a large number of sensor nodes equipped with specialized sensors that can monitor various physical conditions such as pressure, temperature, sound and vibration (Manju et al.,2013). The sensors communicate their data to a base station(sink). The sink node acts as an interface between the network and users, it helps to connect a WSN with the external world. A wireless sensor network can be made up of hundreds of thousands of sensor nodes that can communicate among themselves using radio signals. It is possible to retrieve required data from the network by sending relevant queries to the sink and gathering results from the sink.

A wireless sensor node is equipped with computing devices, sensing, radio transceivers and a power component. Typically, individual nodes in a WSN by nature are resource constrained in terms of limited storage capacity, processing speed and communication bandwidth. When the sensor nodes in a network are deployed, they perform self-organization to form the network through multi-hop communication and the onboard sensors begin to collecting information of interest. The working mode of the sensor nodes may be either continuous or event driven and they have the capacity to respond to queries sent from a control site to perform specific instructions. WSN is assumed to be static and homogeneous with all sensor nodes having the same memory, computational power, except the sink node (Mathew et al., 2015). A lot of research on Wireless Sensor Networks is currently focused on design that will lead to energy efficiency and computationally efficient protocols.

With the increasing use of sensing technologies in emerging networks security weakness in the sensor technology due to their resource constrained limited nature has brought to the attention of many practitioners. However, the limited nature of sensor nodes does not encourage the adoption of security mechanisms, which may leave open vulnerabilities to be exploited (Costa et al., 2017).

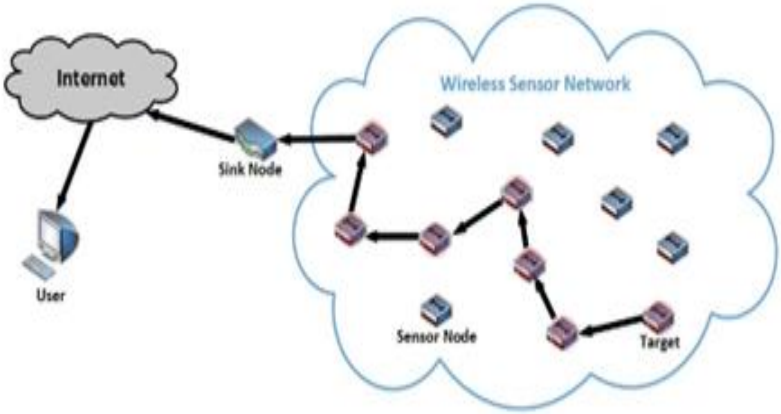


Figure 1: Simple Wireless Sensor Network

2.2.1 Application of Wireless Sensor Networks

Wireless Sensor Networks are becoming increasingly important and are applied in many areas of that affect our lives ranging from military to medical, some of the areas of application are:

Table 1: Summary of WSN application areas

Application	Function	Description
Military Application	Sensing, Target tracking and Event Detection	WSN is used to monitor the resources, track enemies and targets, to assess the damage, detection of attacks such as nuclear, biochemical and track soldier's health status (Saravanakumar et al., 2021)
Environmental Application	Sensing, Event Detection	WSN is used to monitor the weather conditions, soil conditions, in precision agriculture, forest fire detection, and Volcano, Flood and pollution detection (Shaikh et al., 2021)
Home Appliance	Sensing, Event Detection	Sensors are buried in the appliances to help automate. They assist in management and

		monitoring of these appliances locally or remotely (Karthikeyan et al.,2022)
Vehicle Tracking	Target Tracking	Location estimation of vehicles (Upreti et al.,2022)
Structural and Industrial Monitoring Applications	Sensing, Event Detection	To monitor the condition of the structures, bridges, tunnels, machinery used in industry. to estimate wear and tear (Majid et al., 2022)
Business and Inventory Control Applications	Sensing, Event Detection	Inventory monitoring to keep track of the items in the inventories. To check the supply chain system (Hamdy et al., 2022)
Medical Applications	Sensing, Event Detection	The sensors can be implanted or attached to patients to observe the physiological parameters and other conditions and provide appropriate treatment at the right time (Sharma & Singh, 2022)

2.2.2 Characteristics of Wireless Sensor Networks

WSN have the ability to collect the data and the ability to communicate with each other. The sensor nodes used have power consumption constrains as they get their power from batteries. When the sensor node runs out of energy it cannot sense, process or communicate data and for that reason energy consumption is an important factor in WSNs. Energy optimization can be more complex in sensor networks since it involved not only minimizing energy consumption but also prolonging the life of the entire network. It can be achieved through energy awareness focused design and operation.

WSN can be deployed indoors or outdoors and has the ability to withstand harsh environmental conditions. The nodes are portable and can be used to form wireless networks anywhere anytime with great mobility. The nodes are usually low-cost, they make use of simple technology hence they have low processing power and small radio ranges. Other characteristics are Heterogeneity of nodes, Scalability to large scale of deployment and Ease of use cross-layer design (Asha et al., 2016).

2.2.3 WSN Energy Consumption Factor

As far as the sensor network is concerned there are several factors that can lead to energy depletion. In 2012, (Rezaei & Mobininejad, 2012) suggested the following factors:

i. Many sensor nodes sense the same data deployed in a small area.

ii. Sending the repeated sensed data often to the cluster heads also lowers channel utilization.

iii. To send data, a sensor node must keep on listening to the channel.

iv. In periodic sensing, keeping the node “on state” while not in use leads to inefficient use of energy.

v. Collision and retransmission

vi. Sending control packets in large volume needs extra energy especially if the packet is too large.

vii. The need for a greater processing facility in sensor nodes consumes more power.

viii. Same event may sense more than one node due to overlapping regions of area of coverage.

2.2.4 Threats and Challenges Wireless Sensor Networks

Devices used in the Wireless Sensor Networks are of the resource constrained nature hence they are vulnerable to several attacks:

i) **Passive attacks: They involve** eavesdropping and monitoring of data on transit. The objective of the adversary is to obtain data that is being transmitted. Passive attack can be categorized into the release of message contents and traffic analysis. Passive attacks are not easy to detect as they do not involve any modification of the data transmitted. The data is transmitted and received in normal fashion without the sender or receiver noticing any suspicious activity on the traffic pattern. However, in this kind of attack prevention rather than detection is preferred. This prevention can be achieved by use of appropriate encryption techniques.

ii) **Active attacks:** This attack involve modification of the data stream or inclusion of a false stream and come in four different categories:

a) **A masquerade** A masquerade attack is an attack that occurs when an adversary (masquerader) illegally gains access to the identity of an authorized user to gain access to every data the victim is authorized to access (Narwal & Mohapatra., 2021). A masquerade attack will include one of the other types of active attacks such as the **replay attack**. For example, replay attack can capture authentication sequences and replay after a valid user authentication process has successfully taken place, thus enabling an unauthorized entity to impersonate an authorized entity with system privileges (Hou et al., 2018).

b) **Modification of Messages** This form of attack can stem from a masquerade where some portion of a legitimate message that was captured from a legitimate communication is altered and retransmitted in order to produce an unauthorized effect.

c) **Denial of Services (DoS)** prevents or inhibits the normal use or management of communications facilities, this attack can exhaust the resources available to a victim node, by sending extra unnecessary packet and thus prevents it from performing normal operations or degrading its performance (Asha et al., 2016).

2.2.5 Security Requirements for WSNs.

a. **Availability:** Availability ensures that the services or resources offered by the network or a sensor mote will be available whenever required. This can be maintained by regulating the sleeping patterns for a sensor mote.

b. **Integrity:** There are chances that an adversary can make unauthorized changes to data collected by the sensors putting the entire network in disarray. Data can also be unintentionally altered leading to false data usage. Integrity ensures the reliability of the data transmitted. Provides the ability to confirm that a message has not been altered or changed in the network.

c. **Confidentiality:** Confidentiality ensures the concealment of a message from an adversary so that the message communicated in WSN remains confidential to unauthorized persons.

d. **Forward secrecy:** In forward secrecy an assurance is given that a session key derived from a set of long-term public and private key will not be compromised if the private key of one of the parties is compromised. If one message is compromised the previous message will not be affected (Toorani & Shirazi, 2008).

e. **Node Authentication:** The reliability of the message guaranteed if its origin can be identified and is authorized. A wireless sensor node has to prove its validity to other motes in a wireless network and the sink. This avoids the adversary to send malicious information in the network. The base station confirms the authentication of the sensor mote.

f. **Data freshness:** Data freshness ensures that received data/message has not been replayed and should be fresh based on a set time threshold. Data received should have been created recently.

2.2.6 Adopting Cryptographic Schemes for WSN

Traditional cryptographic primitives need to be adopted for use in resource constrained environments.

2.2.6.1 Cryptographic hardware accelerators:

In 2018, (Puttmann et al., 2008) they explored different hardware accelerators for cryptography based on elliptic curves. They were able to provide a multiprocessor system on chip platform that was hierarchical in nature that can be used for fast integration and evaluation of novel hardware accelerators. A coupling on different hierarchy levels of the multiprocessor system on chip platform is provided on the two application scenarios of the hardware accelerators.

A method to implement DTLS using hardware assistance on sensor nodes was proposed by (Kothmayr et al., 2012). There solution assumes that each sensor is equipped with a Trusted Platform Module (TPM) which is an embedded chip that offers secure generation of cryptographic keys and sealed storage as well as hardware support for cryptographic algorithms. The fully authenticated handshake can be performed between a sensor and a subscriber which is another sensor. The subscriber and sensor have to transmit their X.509 certificate for the authentication phase. These certificates are signed by a trusted CA and are included in a fully authenticated DTLS handshake. This solution not only has a high security level by establishing the trusted relationship with the assistance of an approved third party, but it also provides message authentication, integrity and confidentiality with low-cost energy, latency and memory consumption as claimed by the authors.

2.2.6.2 Adopting cryptographic schemes

Adopting existing schemes for use on WSNs has become a more popular technique. (Antipa, et al., 2006) proposed a technique to accelerate verification process of ECDSA signatures and other Elgamal-like signatures with the use of side information to accelerate signature the verification process. In 2016, (Zhong et al., 2016) improved elliptic curve cryptography digital signature scheme for use on WSNs by optimizing the signature generation module of ECDSA. (Zhang et al., 2011) developed a variant of ECDSA which was found by (Sarath et al., 2014) to be more complex and time consuming.

2.3 Computer Security

Basic computer security can be defined within confidentiality, integrity and availability. The three concepts embody fundamental security requirements for both data or information. One of the ways of achieving the three concepts is encryption. In 1999, (Goldreich, 1999) defined security from two perspectives. The first perspective is information theoretic where information is considered insecure if the ciphertext generated contains information about the plaintext. A high level of security can be attained if the secret key used is at least as long as the length of the message transmitted through an encryption scheme. The fact that the key has to be longer than the message, is indeed a drastic limitation on the practical uses of such schemes.

In the second perspective it does not matter whether the ciphertext contains information about the plaintext. It is based on computational complexity where the key concern is whether it is possible for an adversary to extract this information. This approach has the capacity to offer high level security even if the key is shorter than the total length of the message encrypted by a security scheme.

2.3.1 Provable Security

Traditional cryptographic schemes for many years were designed in an ad hoc manner. A cryptographic goal would be defined and then a solution would be given and the scheme would be considered secure if no attacks against it were found. If a new attack was found, the scheme would be either repaired or discarded. If repaired, the scheme can still be subject to possible unforeseen attacks.

Providing proof of security is the most important work in the design of a cryptographic scheme. The security is proofed through a rigorous mathematical framework against computationally bounded attackers.

In the concept of provable security, the approach is to prove that a reduction exists between the difficulty of breaking the designed scheme and the difficulty of solving a hard problem or breaking the security of an underlying cryptographic primitive (Dent, 2006).

Provable security emerged in the 1980s when researchers decided to develop precise definitions for cryptographic schemes and specify appropriate security models for them. According to (Bellare, 1997), the term provable security is misleading as one does not actually prove security of a scheme, but actually provides a reduction of the security of the scheme to the security of a mathematical hard problem or an underlying primitive. Hence, a more appropriate term for this genre of work would be reductionist security. The notion of using reduction arguments to prove the security of cryptographic primitives is very well known and has become standard in most cryptographic research.

The provable security paradigm is as follows:

a. *Cryptographic scheme.* It starts by formally defining the functionality of the cryptographic scheme, specifying the behaviour of each component algorithm. There is a need to consider if the algorithm is probabilistic or deterministic, the values taken as inputs and what the outputs will be and the correctness requirements.

b. *Specify a security model*. A security model will define what a computationally bounded adversary is allowed to do and when, and what it means to break the scheme. The capabilities of an adversary will usually depend on a typical practical use of the cryptographic scheme. The security models can take the form of a game between an adversary A and a challenger C, where C answers oracle queries to A, or the form of an experiment. Experiments are used to model what inputs are given to the adversary and how they are generated. A value of 0 or 1 is returned depending on the output of the adversary and the security of the cryptographic scheme will be measured in terms of the advantage of an adversary in achieving the security goal specified by the game or experiment.

c. *Show a reduction*. Given the underlying primitive or computational hardness assumption it is possible to show that the only way the adversary can break the scheme, with respect to a given security model, will be by breaking its underlying hardness assumption.

2.3.2 Random Oracle Model Versus Standard Model

2.3.2.1 Standard Model

In cryptography, the standard model refers to a computational model where a given adversary can be defined by the computational resources at hand and the cumulative time taken (Dharminder & Mishra, 2020). Security schemes that are proven secure using the complexity assumption are said to be secure in the standard model. Several schemes have been proposed and proven to be secure in the standard model however some of the schemes have been proved not to be secure as initially declared. Some popular and practical secure schemes in the standard model are the signature schemes by (Boneh & Franklin, 2003; Cramer & Shoup, 1999). Security schemes secure in the standard model are computationally more expensive than random oracle-using schemes (Kurosawa & Desmedt, 2004). According to (Koblitz & Menezes, 2015) the concept leads to questionable use of the term “standard” and they found that all of the non-ROM constructions have potential security weaknesses that were not present in the original ROM-versions. In reality adversaries with unlimited computational resources and time do not exist.

2.3.2.2 Random Oracle Model

The concept of Random Oracle Model (ROM) was formalized by (Bellare & Rogaway, 1996) inspired by the need to provide rigorous security proofs for efficient cryptographic primitives. The random oracle H is used as a black box that responds to a query for the hash value of a bit-string M by giving a random value $y = H(m)$. With every query of M, the oracle makes an independent random choice while still keeping a record of its responses and repeats the same response if the same M is queried again.

In the random oracle model, it is assumed that, the hash function is substituted by a random function called random oracle. The random function is allowed access publicly. As a result, in the random oracle model, the hash value cannot be computed by the adversary (Liu et al., 2010). A sequence of games is used when proofing security of m in message space M.

The security for cryptography primitives is typically defined as an attack game played between an adversary denoted by A and an entity called challenger denoted as C who are both probabilistic processes that communicate with each other where the game is modeled in a probabilistic space (Shoup, 2004).

2.3.3 Security Models

In cryptographic schemes the security models can be defined in terms of an adversary who is an efficient algorithm that attempts to break a cryptographic scheme. A security model consists of two main parts: 1) definition of what it means for a cryptographic scheme to be "broken", and 2) the resources an attacker has to gain access. Hence, giving a formal notion of what it means for a cryptographic scheme to be secure. If a cryptographic primitive can be shown to be secure in presence of a powerful adversary then it can hold up to weaker attacks.

The combination of attack goals and capabilities yield different notions of what it means for a cryptographic scheme to be secure. The canonical security models for analysis of public-key encryption and signature schemes are IND-CCA2 and UF-CMA. Formal specifications of what it means for a scheme to be secure under these models is given by the following definitions:

2.3.3.1 Chosen Ciphertext Attack

This form of attack is called an adaptive chosen ciphertext attack and sometimes known as midnight or lunchtime attack (Cramer & Shoup, 1998)**.** The adversary denoted as A is considered to consist of two separate parts or stages conducted by two adversaries. The adversaries are type-I and type-II adversary denoted as A_I and A_{II} respectively and are not allowed to communicate directly. When running A_I, it is given Alice's public key PK_A as input, and returns two messages of its own choice, as well as any state information it wants to pass on to A. One of the messages is then picked at random without the knowledge of the adversary and encrypted with PK_A . The second stage, A_{II}, is run with Alice's public key PK_A, the state information from A and the encrypted ciphertext as input. It returns a single bit, attempting to guess which of the messages had been encrypted. During the entire simulation, the adversary is allowed to query a decryption oracle for any ciphertext, with the restriction that it may not decrypt the challenge ciphertext itself. If the advantage of A at distinguishing between the encrypted messages is negligible in the security parameter k, then the scheme is considered to be secure. When this form of attack is adaptive then it is denoted as CCA-II else it is denoted as CCA-I.

2.3.3.2 Chosen Message Attack

In this form of attack an adversary denoted as A is given Alice's public key PK_A, and attempts to create a message/signature pair (m, s) that is valid under this key. During the simulation, the adversary is allowed to query a signing oracle with any message, with the restriction that (m, s) is considered an invalid forgery if m was ever queried to the oracle. If the success rate of an adversary in creating valid forgeries are negligible in the security parameter k, then the scheme is considered to be secure. This attack is usually denoted as CMA.

2.3.4 Public Key Encryption

Public key encryption also known as asymmetric encryption was introduced 1976 by Diffie and Hellman (Diffie & Hellman, 1976). In their proposed concept, each person makes use of a pair of keys, one called the public key and the other called the private key. The public key is kept in the public domain while the private key is kept as a secure secret. The key distribution problem is solved since all communications require only public keys and not the private key. If two parties are communicating, let’s call them Alice and Bob. When Alice wants to transmit a secret message to Bob, she looks up Bob's public key in a public directory, then uses it to encrypt the message and sends it Bob. Bob on the other hand will make use of his private key to decrypt the message and read it. No adversary listening in can be able to decrypt the message. The concept of public key encryption enables anyone to send an encrypted message to Bob but only Bob can read it.

2.3.5 Hash Functions

Cryptographic hash functions can be used for many purposes; the most common use of hash functions is data integrity. The characteristic nature of a cryptographic hash function makes it a good tool for checking integrity of a message. Cryptographic hash functions are collision resistant, one-way and have a fixed length output.

According to (Tchórzewski & Jakóbik, 2019), applications of hash functions may include message integrity checking, digital signatures, authentication procedures and other information security related applications. Cryptographic hash functions map an arbitrary-length message string to fixed-size message string called hash value. Hash function H is required to be one-way and collision resistant. It is one-way if it is computationally impossible if, given hash value $x = H(M)$ it is not possible to recover message M and is collision resistant only if no program can find a collision in H. A formal definition of a hash function is given as follows:

A hash function is a function $H: D \longrightarrow R$, where the domain $D = \{0,1\}^*$ and the range $R = \{0,1\}^n$ for some $n \geq 1$ while a keyed hash function is defined as: A keyed hash function is a function $H_k: D \longrightarrow R$, where $K = \{0,1\}^k$ is the key space and $R = \{0,1\}^n$ for some $n \geq 1$.

Characteristics of a cryptographic hash function

a) *Collision resistance:* Hash function H is collision resistance if it is difficult to find x,$x' \in D$ such that $x \neq x'$ and $H(x) \neq H(x')$.

b) *Preimage resistance:* Hash function H is preimage resistance if given $r_R \in R$ it is difficult to find $x \in D$ such that $H(x) = r$.

c) Second preimage resistance: Hash function H is second preimage resistance if given if given $x \in D$ it is difficult to find $x' \in D$ such that $x \neq x'$ and $H(x) \neq H(x')$.

2.4 Approaches for optimizing security schemes

2.4.1 Hybrid approach

This approach requires a scheme to be composed of both asymmetric and symmetric scheme. With the need for improving the security systems for the WSN, (Abdullah et al., 2018) proposed a hybrid security protocol for WSN. In 2019, (Bhushan & Sahoo, 2019) proposed an Integrated IDS scheme (IIS) that integrates clustering along with digital signature for efficiently securing WSNs. There scheme employs symmetric cryptography to ensure efficient data security.

To ensure lightweight signcryption, (Yu & Yang, 2017) applied the technique of certificateless hybrid signcryption to an elliptic-curve cryptosystem, and construct a low-computation certificateless hybrid signcryption scheme. While (Iqbal et al., 2019) provided a heterogeneous online/offline signcryption for WSNs. Other schemes that have combined advantage of two or more cryptographic primitives have been proposed as discussed in (Sivasundari & Ramakrishnan, 2019; Mohamed et al., 2020).

2.4.2 Tailored Approach

Tailoring allows a security scheme to be modified to efficiently work in an identified environment. Many traditional schemes have been modified to work in resource constrained environments such as WSN. (Venkataraman & Sadasivam, 2019) proposed an efficient digital signature scheme where the computational cost of the original ECDSA was reduced by removing inverse operation in both key generation and the signing algorithm. The security of scheme is guaranteed through the process of hidden generator point concept.

In 2016, (Li et al., 2016) also gave a certificateless signcryption scheme by modifying the scheme by (Barreto et al., 2008). Their proposed access control scheme was able to satisfy ciphertext authenticity and public verifiability. The research approach intents to use the modified approach to achieve an efficient signcryption scheme for wireless sensor networks.

2.5 Public Key Cryptography

The proposal of public-key cryptography is one of the greatest in the history of cryptography. In the early days and perhaps to the current times, all cryptographic schemes have been based on the simple tools of permutation and substitution. (Diffie & Hellman, 1976) are the first to propose the theory of public key cryptography. Mathematical functions are the foundation of public-key algorithms and permit the use of two separate keys as compared to private key encryption, which uses only a single key.

2.5.1 Characteristics of Public Key Cryptosystems

Public Key Cryptosystems to be effective they exhibit the following characteristics:

i. It makes it impossible to recover the decryption key given only access to the cryptographic algorithm and the encryption key.

ii. Any of the two mathematically related keys can be used for encryption, with the other used for the purpose of decryption

2.5.2 Public Key Infrastructure

Public Key Infrastructure denoted as PKI is the common method used to authenticate public keys. In PKI system, Certificate Authority who is a trusted party who is responsible for establishment and verification of the authenticity of public keys. A typical PKI consist of the following components: Certificate Authority (CA), Registration Authority (RA), Certificate repository and certificate management system.

The CA creates, manages, stores, distributes and revokes digital certificates. CA might be a part of creating public key pairs and sending it to a user over a secure channel. The CA binds public key with respective user's identities through a digital signature with its private key and stores it in a repository. Users can also create their own public key pair and transfer them to the CA through a secure channel then the CA creates the required certificates. CA must verify the identity of the user before granting

corresponding public-key certificates, in a WSN a base station can perform the work of a CA. The RA performs initial authentication and acts as the verifier for the CA before a digital certificate

is issued to the user. Certificate repository is basically a directory where certificates with their public keys and Certificate Revocation Lists are stored. The fact that PKI is inefficiency in terms of computation it makes it impractical for use in WSN.

2.5.3 Identity-Based Cryptography

In 1984, (Shamir, 1984) introduced the notion of Identity based cryptography but until 2001 it was an open problem (Mandal et al., 2016). In 2003, (Boneh & Franklin, 2003) presented the first practical Identity Based Encryption (IBE) using bilinear pairing over elliptic curves.

The ID-Based cryptography reduces the requirement of public key certificates with the help of a trusted third party known as a public key generator (PKG) whose role is to generate and issue private keys of all of its users so that only these users can decrypt the ciphertext and that provides the implicit in certification. Hence, it reduces the space and time complexity which makes the solution advantageous especially for WSNs (Nguyen et a., 2015).

Indeed, any sensor nodes can generate the public key of other nodes when needed to establish a secure communication using their identities. In addition, the revocation mechanism is supported by consulting the list of valid sensor identities. Though advantageous, ID- based schemes are still vulnerable to key-escrow attacks because the PKG knows the private keys of all communicating nodes within the network. It can masquerade as any node and consequently intercept all the communication in the system.

2.5.4 Certificateless Cryptography

In 2003, (Al-Riyami & Paterson, 2003) introduced the concept of certificateless public key cryptography (CL-PKC) to address the issue of key escrow while still avoiding use of certificates where the private key is partitioned into two partial keys. A trusted third party known as a key generator center (KGC)takes the user's identity together with a master secret key as input and generates a partial private key and forwards the partial private key to a valid user. The user will choose a random secret value and combine the random secret value with the partial private key to generate a secure full private key. The user's public key is no longer computable from the identity of the user. If a sender wishes to send a message to a designated receiver in certificateless environment, the sender has to obtain the correct public key of the designated receiver. However, it does not require the authentication of receiver's public key and no need of the certificates. The cost efficiency of certificateless signcryption can be very useful in areas such as wireless sensor networks, mobile ad hoc networks among other areas (Mandal et al., 2016).

2.6 Mathematical Background of Elliptic Curve Cryptography

Elliptic curves are applied in diverse areas of mathematics, this can range from complex analysis to number theory and cryptography. Elliptic Curve Cryptography (ECC) is a public key cryptosystem that was independently discovered by Victor Miller (Miller, 1985) and Koblitz (Kobiltz, 1987) in 1985 as an alternative mechanism for implementing public key cryptography.

EC cryptosystems are equivalents of existing public-key cryptosystems in which modular multiplication is replaced by elliptic curve addition operation. One can construct elliptic curve encryption, key agreement and signature schemes by making analogs of DSA, El-Gamal and Diffie-Hellman.

An elliptic curve can be defined by an equation with two variables with coefficients. In cryptography, coefficients and variables are restricted to use of only elements in a defined finite field, this results in a defined finite abelian group. They are referred to as finite abelian group since they are described by used of cubic equations, more similar to those used for computing the circumference of an ellipse. In elliptic curves a cubic equation can take the following form, known as a Weierstrass equation:

$$y^2 + axy + by = x^3 + cx^2 + dx + e \qquad (1)$$

where values *a*, *b*, *c*, *d* and *e* are real numbers and both *x* and *y* take on values in the real numbers. It is sufficient to limit ourselves to equations of the form:

$$y^2 = x^3 + ax + b \qquad (2)$$

Such equation is said to be cubic because the highest exponent is 3. Elliptic curves also contain a point of infinity denoted as *O*. Figure 2 shows an example of elliptic curves.

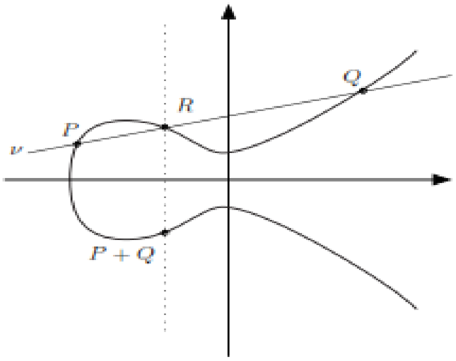


Figure 2: Elliptic Curve

It can be shown that a group can be defined based on the set E (*a*, *b*) for specific values of *a* and *b* in Equation 2, provided the following condition is met:

$$4a^3 + 27b^2 \neq 0 \qquad (3)$$

The condition Δ ≠ 0 is used to ensure the smoothness of the elliptic curve, that is, there are no points at which the curve has two or more distinct tangent lines. To define the group, an operation is defined, called addition and denoted by +, for the set E (*a*, *b*) which is an abelian group, where *a* and *b* satisfy Equation 3. In geometrically, the rules applied for addition are stated as follows: If there are three points on an elliptic curve that exist on a straight line, their sum is set as *O*. With such knowledge, one can now define the rules that can be applied in addition over an elliptic curve.

2.6.1 Finite Fields

A finite field is composed of a finite set of elements that together with two operations of binary referred to as addition and multiplication that satisfy certain given set of arithmetic properties (Johnson et al., 2001). The number of elements in the field is known as the order of a finite field.

2.6.1.1 Finite Field of the form $\boldsymbol{GF_p}$

The finite field F_p can be defined as a prime finite field containing p elements. The elements of F_p are represented by the set of integers:

$$\{0,1,\ldots,p-1\}$$

Where addition and multiplication are defined as

i. **Multiplication**: if $a, b \in F_p$, then $a \cdot b = c$ in F_p where $c \in [0,1,\ldots,p-1]$ is a reminder when integer $a \cdot b$ is divided by p, i.e $a \cdot b \equiv c \; mod \; p$. Multiplicative identity is integer 1.

ii. **Addition**: if $a, b \in F_p$, then $a + b = c$ in F_p where $c \in [0,1,\ldots,p-1]$ is a reminder when integer $a + b$ is divided by p, i.e $a + b \equiv c \; mod \; p$. Additive identity is integer 0.

2.6.1.2 Finite Field of the form $\boldsymbol{GF}(_{2^m})$

The use of Finite FieldF_{2^m} implies 2 finite field containing 2^melements with $m \geq 1$. The set of integers modulo 2^m for ≥ 1 is not a field. Elements of F_{2^m} should be represented by the set of binary polynomials of degree $m-1$ or less.

$$\left\{a_{m-1}x^{m-1} + \cdots + a_{m-2}x^{m-2} + \cdots + a_1x + a_0 \colon a_i \in \{0,1\}\right\}.$$

Multiplication and addition and defined in terms of irreducible binary polynomial $f(x)$ of degree m referred to as reduction polynomial.

i. Multiplication: if $a = a_{m-1}x^{m-1} + \cdots + a_0, b = b_{m-1}x^{m-1} + \cdots + b_0 \in F_{2^m}$, then $a \cdot b = c$ in F_{2^m} where $c = c_{m-1}x^{m-1} + \cdots + c_0$ is the reminder when the ab is divided by $f(x)$ with all the coefficient arithmetic performed in modulo 2.

ii. Addition: if $a = a_{m-1}x^{m-1} + \cdots + a_0, b = b_{m-1}x^{m-1} + \cdots + b_0 \in F_{2^m}$, then $a + b = c$ in F_{2^m} where $c = c_{m-1}x^{m-1} + \cdots + c_0$ with $c_i \equiv a_i + b_i \; (mod \; 2)$

2.6.2 Abelian

An abelian group G sometimes denoted by{G,·} is a set of elements with binary operation denoted by{·} that associates to each ordered pair(a, b) of elements in G an element$(a \cdot b)$ in $G,$ in such a way that the following axioms are observed.

i. Closure, if $a\ and\ b$ belong to G, then $a \cdot b$is also in G.

ii. Associative $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c in G.

iii. An Identity element is an element e in G such that $a \cdot e = e \cdot a = a.$

iv. An Inverse element for each a in G there is an element a' in such that $a \cdot a' = a' \cdot a = e$

v. Commutative$a \cdot b = b \cdot a$ for all $a, b\ in\ G.$

2.6.3 Elliptic Curves

Elliptic Curves over F_{2^m}

F_{2^m} is characterized by 2 finite field and $a, b \in F_{2^m}$ satisfy $b \neq 0$. where the curve $E(F_{2^m})$ over F_{2^m} is defined by parameters $a, b \in F_{2^m}$. The equation:

$y^2\ mod\ p = x^3 + ax^2 + b$ in F_{2^m} is used together with extra point called infinity represented by o.

Elliptic Curves over *Fp*

Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field for a prime curve over F. A cubic equation always used in such a way that the variables and coefficients take on values within the set of integers from 0 through $p - 1$ and in which calculations are performed modulo p

For elliptic curves over F_p , as with real numbers, a limit is set to equations of the form of Equation 2, but in this case with coefficients and variables limited to F_p as shown equation 4.

$$y^2 \; mod \; p = x^3 + ax + b \; mod \; p \qquad (4)$$

It comes with an extra point called infinity represented by o and integers $a, b \in F_p$ should satisfy $4 \cdot a^3 + 27 \cdot b^2 \not\equiv 0 \; (mod \; p)$.

Elliptic Curves requires much smaller keys compared to other primitives as shown by Table 2, this directly translates to important savings in bandwidth and memory requirements making it most preferred for the development of cryptographic primitives for resource constrained devices.

Table 2: Key sizes for ECC and RSA for equivalent security levels

Cryptosystem	KeySize (bits)				
ECC	160	224	256	384	512
RSA	1024	2048	3072	7680	15360

To create a cryptographic system using elliptic curves, one needs to find a "hard problem" corresponding to factoring the product of two primes or taking the discrete logarithm. Consider equation $Q = wP$ where $Q, P \in E_p(a, b)$ and $w < p$. It is relatively easy to calculate $Q \; given \; w \; and \; P$ but it is hard to determine $w \; given \; Q \; and \; P$ and this is what is called discrete logarithm problem for elliptic curves.

Consider the group $E_{23}(9,17)$. This is the group defined by the equation $y^2 mod \; 23 = (x^3 + 9x + 17) \; mod \; 23$. What is the discrete logarithm w of $Q = (8,7)$ to the base $P = (16,5)$?. The simplest approach is to use brute force through multiples of P until Q is found as shown below:

$P = (16,5); 2P = 920,20); \; 3P = (4,14); 4P = (19,20); 5P = (13,10); \; 6P = (7,3); 7P = (8,7)$because $7P = (8,7) = Q$ therefore $w = 7$ however, in real application w would be a large number that cannot be discovered through brute-force technique.

2.6.4 Group law for elliptic curves

According to (Fang et al., 2017) group law for elliptic curves define a group over elliptic curves where:

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

ii. The identity element is the point at infinity$o$;

iii. Addition is given by the following rule: given three aligned, non-zero points P, Q and R, their sum is $P + Q + R = O\ P + Q = -R$. This operator is both associative and commutative, $P + (Q + R) = (P + Q) + R = Q + P + R = O$. An abelian group based on the points set over elliptic curve is achieved.

iv. The inverse of point P is the one symmetric about the *x*-axis. Assume that P(*x*, *y*),$Q(x_2, y_2)\ \in E_p(a, b)$, the reverse of point $P$is $-P, -P = (x, -y)$ and $P + O = P, P + (-P) = O, Q - P = (x_2, y_2\ ) - (x, y) = (x_2, y_2) + (x, -y)$.

2.6.5 Point Addition

Point addition is when two distinct points are added on the elliptic curve to get a third point, which by virtue of its group property, lies on the curve too. The addition of points on an elliptic curve is defined by Chord and Tangent rule. Let $P = (x_1, y_1)\ Q = (x_2, y_2)$be two distinct points on anelliptic curveE where$R = P + Q\ and\ P + (-P) =\ O$. The sum R, of Q and P, is defined as follows: Draw a line connecting P and Q extend it to intersect the elliptic curve at a third point. The negative of the third point is given as the sum of R. The negative of a given point is defined by reflecting the point on the x-axis. The double R, of P, can be defined as follows: When the tangent line to the elliptic curve at P is drawn, allow it to intersect the elliptic curve at given a second point. Then the double R is the reflection of this point about the x-axis.

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2\ and\ y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1. \qquad (5)$$

2.6.6 Point Multiplication

Point Multiplication also known as scalar multiplication is the arithmetic operation which computes kP where k is an integer and P is a point on elliptic curve. It is done by repeated addition. For example, $Q\ = kP$means Q is obtained by adding Pk times to itself $(p\ +\ p\ +\ p.\dots k\ times)$. Cryptanalysis involves determining $k\ given\ P\ and\ Q$. This is a dominant operation in the execution time of elliptic curve cryptographic schemes.

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \ and \ y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1. \qquad (6)$$

2.6.7 Point Doubling

This is an operation that returns to the case where you find the point R on a curve such that $R = 2P$. Coordinates of R can be obtained by employing the following formulas:

$s = \frac{3p_x^2+a}{2p_y}$, $R_x = s^2 - 2p_x$ and $R_y = s(p_x - r_x) - p_y$. (7)

2.6.8 Elliptic Curve Computational Assumptions

In elliptic curve cryptography, security relies on the hardness assumption used in the design of the cryptographic scheme. Below are some computational assumptions used in cryptography:

Definition 2.6.8.1 (ECDLP): Let G be a cyclic group and P be its generator of order q. Given $< P, aP > \in G$ for unknown $a \in Z_q$. If A is a PPT adversary its advantage in solving the ECDLP is defined as $Adv^{ECDLP}(A) = Pr[A(P, aP) = a | a \in Z_p$

The ECDL assumption is that for any PPT adversary A the above advantage is negligible.

Definition 2.6.8.2 (CDH): Computational Diffie-Hellman problem**.** Given $< P, aP, bP >$ $\in G$ for unknown $a, b \in Z_p^*$ $t$he computational deffie hellman problem is determined by $abP \in G$

If A is a PPT adversary its advantage in solving the CDH is defined as $Adv^{CDH}(A) = Pr[A(P, aP, bP) = abP | a, b \in Z_p$. The CDH assumption is that for any PPT adversary A the above advantage is negligible.

Definition 2.6.8.3 (DDH): Decisional Diffie-Hellman problem. Given $< P, aP, bP, cP >$ $\in G$for unknown $a, b, c \in Z_p^*$. Returns true if $ab \equiv c \ mod \ p$

Definition 2.6.8.4 (GDH): Gap Diffie-Hellman problem. Given that the DDH problem is easy in G, solve an instance of the CDH problem $< P, aP, bP > \in G$.Let G be a cyclic group and P be its generator of order q. Given $(aP, bP, cP) \in G$ for unknown $a, b \in Z_q$.

With the help of DDH oracle which on input (aP, bP, cP) outputs 1 if $c \equiv ab \bmod q$, else it outputs 0.

Definition 2.6.8.5 (W-DH): Weak Diffie-Hellman problem. Given instance $< P, Q, sP >$ $\in G$ and some $s \in Z_p^*$ the output sQ is considered.

2.7 Digital Signatures

Digital signatures form the core of secure digital communications. The idea of digital signatures based on asymmetric cryptography was put forward by (Diffie & Hellman, 1976). A digital signature is a cryptographic primitive used to proof data origin authentication, non-repudiation and data integrity. The idea behind digital signature is to give an electronic means for replacement of handwritten signatures. Digital signatures provide an assurance to the receiver that the data received was transmitted by the assumed party. Data integrity plays an important role in virtual platform. It is important to protect data from unauthorized alteration and digital signatures provide us with the means to verify data received from a sender.

In public key cryptography, a digital signature is constructed from two different digital keys commonly known as a key pair. Each key pair is composed of a private key only known by the signer and a public key that the intended recipient must have knowledge of. The two keys are mathematically related but can be used separately. The algorithm works in such a way that it is computationally impossible for a third party to recover the private key given a user’s public key. Figure 3 by (Kerry, 2013) show a general message signing and verification process.

With the current technological advancements, digital signatures are used in various digital platforms to validate data ownership and authenticity. The use of digital signatures is becoming widespread. A well designed digital signature scheme can expedite the process of maintaining the obligation of the digital signatures in justice. Digital signature assures the traceability of electronic transactions during authentication process (Butun and Demirer,2013).

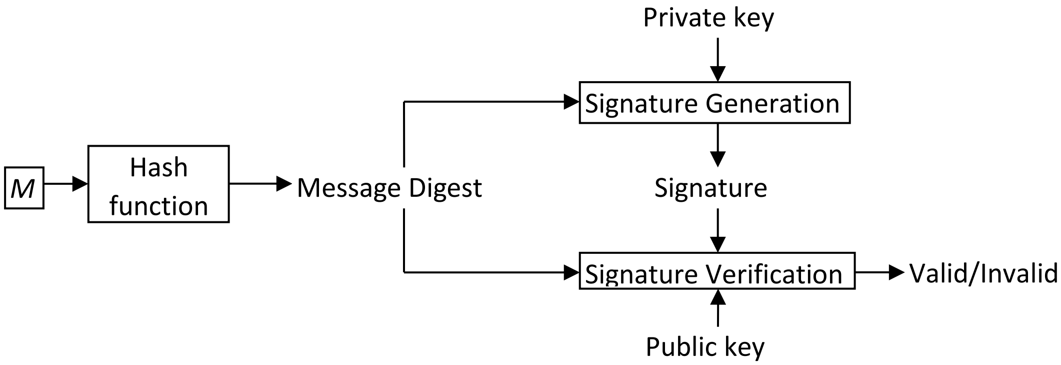


Figure 3: Digital Signature Process (Kerry, 2013)

2.7.1 Digital Signature Framework

Digital signature is defined by a tuple $algorithms(SetUp_{DS}, KeyGen_{DS}, S_{DS}, V_{DS})$ defined as follows:

a. $SetUp_{DS}$: This setup algorithm that takes as input a security parameter 1^k and outputs necessary public parameters.

b. $KeyGen_{DS}$:Key Generation Algorithm, is a probabilistic-time algorithm which on input a security parameter k, produces pair(P, S) where P is called a public key (pk) and S is a secret key that are used in the signing and verification algorithm.

c. S_{DS} (sk, m): Signing Algorithm $\sum$, with public domain parameters and a private key in hand the signing algorithm receives a message m and the private key sk, and outputs a signature σ= $\Sigma_{sk}(m)$

d. $V_{DS}(pk, m, ϭ)$: Verification Algorithm V_{DS} which receives a candidate signature σ, a message *m* and a public key *pk* and returns an answer as to whether the signature for the message *m* is valid or not.

2.7.2 Digital Signature Requirements

a. A Digital Signature must be derived from the message signed.
b. Must be relatively easy to produce a digital signature.
c. Must use information that is unique to the person signing.
d. Must be easy to recognize and anyone can verify the signature.
e. Must be difficult to forge a new message for existing digital signature and a fraudulent digital signature for a given message.

2.7.3 Signature Mathematical Problem

Modern day digital signatures can be classified according to the high underlying mathematical problem, which provides the basis for their security:

Definition 8 Integer Factorization (IF) problem: Given parameters *n, p* and *q*. where *p* and *q* are two large prime numbers it is easy to compute the product *n*, *n=pq* however, given *n*its not easy to factor the product n to arrive at values for *p* and *q*. The RSA digital signature schemes that fall under this classification.

Definition 9 Discrete Logarithm Problem**:** Let q be a prime number and a be a non-zero integer. given a^k mod q an adversary must determine *k* given a and a^k, this is the discrete logarithm problem.

Definition 10 Elliptic Curve Digital Logarithm Problem**:** Let E be an Elliptic curve defined over a finite field F_q, a point $P\epsilon E(F_q)$ of order n and a point $Q \in (P)$. Find the integer k∈ $[0, n-1]$ such that $Q = kP$. Integer l is called the discrete logarithm of Q to the base P which is denoted as k=Q .

2.7.4 Signatures and Hash functions

A cryptographic hash function is a polynomial-time function denoted as $H: \{0,1\}^* \rightarrow \{0,1\}^n$and is used to map a message of arbitrary length to a string of a fixed length some times referred to as a message digest or hash value. A hash function required to satisfy the following characteristics:

Pre-image resistance: Given a hash value $y \in Y$, it should be infeasible to find a preimage $x \in X$ such that $h(x) = y$.

Second Preimage resistance: Given element $x_1 \in X$, it should be impossible to find a different element $x_2 \in X$ such that $h(x_1) = h(x_2)$. Note that there exists minimum difference between preimage resistance and second preimage resistance. The difference can be significant from a practical point of view. Hash functions have an output rule that limits the latitude of an adversary in hash computation, making it more difficult to avoid. The first preimage attack will need to overcome these complexities, while the second preimage attack has an opportunity to copy the parts from the challenge message.

Strong collision resistance: It is infeasible to find two elements $x_1, x_2 \in X$ such that $h(x_1) = h(x_2)$.Note that this is not the same as second preimage resistance as here, both $x_1$and x_2 can be chosen by the adversary.

2.7.5 RSA

The RSA algorithm was developed in the year 1977 by Ron Rivest, Adi Shamir and Leonard Adelman at the Massachusetts Institute of Technology. RSA algorithm is based the concept factorization of numbers, the larger the sequence of numbers you have, the more you are protected. RSA is a cryptographic primitive used to encrypt or decrypt data it also has the capacity to sign and verify messages. In RSA the security of the signature and encryption is dependent on the choice of cryptographic hash function used to compute the signature.

2.7.6 Digital Signature Algorithm

The Digital Signature Algorithm (DSA) relies on the strain of computing discrete logarithms and is based on schemes originally presented by Elgamal and Schnorr. The strengths of DSA over the Elgamal digital signature scheme are that the digital signature is 320-bit long and is not susceptible to some attacks that are a threat to the Elgamal signature scheme. The main weakness of the discrete logarithm attacks is that a scheme based on the hardness can be vulnerable if the ephemeral key is reused.

2.7.7 Elliptic Curve Digital Signature Algorithm

In 1985 a signature scheme known as The ElGamal (Elgamal, 1985) was developed as the first Discrete Logarithm-based signature scheme. In 1989, using the Fiate heuristic based on zero knowledge (Schnorr, 1989) proposed a zero-knowledge identification scheme. In (Nyberg et al., 1994) a new digital signature scheme DSA was proposed, the scheme was based on a mixture of Schnorr and the ElGamal schemes. Their scheme was later modified to the Elliptic Curve Digital Signature Algorithm (ECDSA) under the elliptic curve setting.

The security of ECDSA is pegged on the hardness of Elliptic Curve Discrete Logarithm Problem (ECDLP) which has become popular over the past decade. The use of elliptic curve as its base has made it harder than the DLP and the factoring problem used in RSA based schemes. In ECC a scalar point multiplication given by $Q = dP$ where $Q\ and\ P$ are two points on a given elliptic curve. Finding the value of d is a harder problem since point multiplication is meant to act as a one-way function (Barekar & Hande, 2012).

The harder problem is the ECDLP occurs when the coordinates of $Q\ and\ P$ on a given elliptic curve are known and the value of d needs to be computed. This ECDLP problem becomes harder as the size of domain parameters continue to increase. According to (Faquih et al., 2015) the size of the underlying finite field is larger than 160 bits the computation of ECDLP becomes computationally infeasible and the security of the original ECDSA is rooted on the complexity of the discrete logarithm problem (Braun & Kargl, 2007).

Table 2 compares security strength of RSA and ECDSA in terms of key length given the same level of security. In ECDSA each signer must generate two of keys, one private and one the other public. The signer generates the two keys by first selecting a random integer, $d \in_R [1, n - 1]$ and computes $Q = dG$ which is a point in elliptic curve, the sender's public key is Q and private key is *d.*

The process of signature generation and signature verification in the Elliptic Curve Digital Signature Algorithm is shown in Algorithm 1 and Algorithm 2 below:

Algorithm 1 ECDSA- Digital Signature Generation

```
1. Select a random or pseudorandom integer $k, k \in_R [1, n-1]$
2. Compute point $P = (x, y) = kG$ and $r$ =$x$ mod $n$. If $r$ = 0 then goto step 1
3. Compute $e$ = H($m$), where H is the SHA-1 hash function
4. Compute $s = k^{-1} (e + dr)\ modn$. If $s$ =$O$ then goto step 1
5. Return (r,s)
```

Algorithm 2 ECDSA- Digital Signature Verification

```
1. Verify that $r$ and $s$ are integers in the range 1 through $n$ - 1
2. Using hashing algorithm, compute the 160-bit hash value $e$ = H($m$)
3. Compute $w$ =$s^{-1}$ mod $n$
4. Compute $u_1 = ew$ and $u_2 = rw$
5. Compute the point $X = (x_1, y_1) = u_1G + u_2Q\ If\ X = 0$, reject the signature
6. Compute $v = x_1 mod\ n$
Accept signature only if v=r
```

2.8 Signcryption

Security is a mandatory feature in all forms of digital communication. When sending a message, it is important to ensure authenticity, confidentiality, integrity and non-repudiation can be achieved through communication. Other features increasingly becoming desirable in digital communication are forward secrecy and public verifiability. These features can effectively be achieved through the concept of encryption and digital signature.

Signcryption is a public key cryptographic primitive that is able to achieve both the functionality of signing and public key encryption in a single logical step (Nayak, 2014). The traditional process of signing then encrypting a message has been found through research to be inefficient in terms of number of bits generate, computational operations and size of the entire package (Zheng, 1997).

In the signcryption scheme, the sender generates a ciphertext of the message. The sender sends the ciphertext to the intended recipient. When the recipient receives the ciphertext, he derives the original message through his private key. The cost of computing drastically reduces compared to the traditional signature-then-encryption approach (Zheng, 1997, Singh & Vaisla, 2014). A signcryption scheme should always produce a ciphertext that is much shorter than the traditional combination of a digital signature and public-key encryption ciphertext.

2.8.1 Formal definition of a Signcryption scheme

Definition 2.8.1.1 (Signcryption): A signcryption scheme was introduced by (Zheng, 1997) and it can be defined as a tuple of four probabilistic polynomial time (PPT) $algorithms$ $(Setup, KeyGen, Signcrypt, Unsigncrypt)$ with the following functionalities:

i. $Setup(k) \rightarrow params$. Given security level parameter k, this algorithm will output system parameters $params$.

ii. $KeyGen(params) \rightarrow (SK_S, PK_S), (SK_R, PK_R)$. The public and private key for both sender and receiver are generated by this algorithm.

iii. $Signcrypt(params, SK_S, PK_S, PK_R, M) \rightarrow \sigma$ **or** $\perp$ Given the public key and the full secret key of the sender, the public key of the receiver and a message M, this algorithm will return either a ciphertext σ or error $\perp$.

iv. $Unsigncryption(params, SK_R, PK_S, PK_R, \sigma) \rightarrow M'$. Given the ciphertext σ, the public key of both sender and receiver, private keys of the receiver, the algorithm return message M' or error $\perp$.

In a signcryption application the number basic algorithms affect the corresponding computation and implementation complexity and may cause the signcryption application not to be applicable in some resources-constrained environments such as embedded systems, sensor networks, and ubiquitous computing. Motivated by this, a lot of research work is currently focused on development and implementation of lightweight primitives for resource constrained environments.

The conventional signcryption users are required to choose their own private keys and compute corresponding public keys then submit them to a Certificate Authority (CA) for issuance of digital certificates. This creates a need for digital certificate management infrastructure known as public key infrastructure (PKI) which can be cumbersome to maintain. Signcryption can offer two main security features: confidentiality and unforgeability. The two main security features can be defined depending on whether the adversary is an insider or outsider.

Definition 2.8.1.2 (Outsider IND-CCA2): Let $A = (A_1, A_2)$be an adversary against the confidentiality of signcryption scheme with security parameter k. Confidentiality of the signcryption scheme can be defined via IND-CCA2 security game as follows:

$PP \leftarrow Setup(1^k)$

$(pk_S^*, sk_S^*) \leftarrow KG_S(1^k)$

$(pk_S^*, sk_S^*) \leftarrow KG_R(1^k)$

$(m0, m1, \omega) \leftarrow A_1^{O_S,O_U}(pk_S^*, sk_S^*)$

$C^* \leftarrow SC(pk_R^*, sk_S^*, m_f)$

$if |m_0| \neq |m_0| \; then \; C^* \leftarrow \perp$

$f' \leftarrow A_2^{O_S,O_U}(C^*, \omega)$

$Output \; f'$

Where signcryption oracle O_S and the unsigncryption oracle O_U are defined as $O_S(pk_R, m) = SC(pk_R, sk_S^*, m)$ and $O_U(pk_S, C) = USC(pk_S, sk_R^*, C)$

With the condition A2 cannot query $O_U(pk_S^*, C^*)$. The advantage of the attacker can be defined as

$$Adv_A^{out-IND}(k) = |Pr[EXPT_A^{out-IND-1}(k) = 1] - Pr[EXPT_A^{out-IND-0}(k) = 1]|.$$

The signcryption scheme is said to be outsider IND-CCA2 secure if $Adv_A^{out-IND}(k)$
Is negligible in k for every PPT adversary A.

Definition 2.8.1.3 (Insider IND-CCA2): $Let \; A = (A_1, A_2)$be an adversary against the confidentiality of signcryption scheme with security parameter k. The insider confidentiality of the signcryption scheme can be defined in the following security game:

$PP \leftarrow Setup(1^k)$

$(pk_R^*, sk_R^*) \leftarrow KG_R(1^k)$

$(m0, m1, pk_S^*, sk_S^*, \omega) \leftarrow A_1^{O_U}(pk_R^*)$

$C^* \leftarrow SC\left(pk_R^*, sk_S^*, m_f\right)$

$if |m_0| \neq |m_0|\ then\ C^* \leftarrow \perp$

$f' \leftarrow A_2^{O_U}(C^*, \omega)$

$Output\ f'$

Where the unsigncryption oracle O_U is defined as $O_U(pk_S, C) = USC(pk_S, sk_R^*, C)$ and adversary A_2cannot query $O_U(pk_S^*, C^*)$. The advantage of the adversary can be defined as $Adv_A^{in-IND}(k) = |Pr[EXPT_A^{in-IND-1}(k) = 1] - Pr[EXPT_A^{in-IND-0}(k) = 1]\ |$.

The signcryption scheme is said to be secure against insider IND-CCA-2 if $Adv_A^{in-IND}(k)$ is negligible in k for every PPT adversary A. The adversary has knowledge of sender's secret key and the should be attacking the receiver's keys.

Definition 2.8.1.4 (Outsider UF-CMA): Let A be a PPT adversary against the integrity of a signcryption scheme with security parameter k. Then the outsider unforgeability of the signcryption scheme is captured via the following securitygame.

$PP \leftarrow Setup(1^k)$

$(pk_S^*, sk_S^*) \leftarrow KG_S(1^k)$

$(pk_R^*, sk_R^*) \leftarrow KG_R(1^k)$

$C^* \leftarrow A^{O_S, O_U}(pk_R^*, sk_S^*)$

$Output\ 1\ if$

$m_0 \neq \perp\ for\ m^* \leftarrow USC(pk_S^*, sk_R^*, C^*)$

Else $Output\ 0$,

Where signcryption oracle O_S and the unsigncryption oracle O_U are defined as

$O_S(pk_R, m) = SC(pk_R, sk_S^*, m)$ and $O_U(pk_S, C) = USC(pk_S, sk_R^*, C)$

The adversary's advantage can be defined as

$$Adv_A^{out-UF}(k) = Pr\ Pr\ [EXPT_A^{out-UF}(k) = 1]\,.$$

The adversary is not allowed to query $O_S(pk_R^*, m)$

The signcryption scheme is said to be secure against insider UF-CMA if $Adv_A^{out-UF}(k)$

is negligible for every PPT adversary.

Definition 2.8.1.5 (Insider UF-CMA): Let A be a PPT adversary against the integrity of a signcryption scheme with security parameter k. Then the insider unforgeability of the signcryption scheme is captured via the following security game.

$PP \leftarrow Setup(1^k)$

$(pk_S^*, sk_S^*) \leftarrow KG_S(1^k)$

$(pk_R^*, sk_R^*, C^*) \leftarrow A^{O_S}(pk_S^*)$

$Output\ 1\ if$

$m_0 \neq \perp\ for\ m^* \leftarrow USC(pk_S^*, sk_R^*, C^*)$

Else $Output\ 0,$

Where signcryption oracle O_S is defined as $O_S(pk_R, m) = SC(pk_R, sk_S^*, m)$

The adversary's advantage can be defined as

$$Adv_A^{in-UF}(k) = Pr\ Pr\left[EXPT_A^{in-UF}(k) = 1\right].$$

The adversary is not allowed to query $O_S(pk_R^*, m)$

The signcryption scheme is said to be secure against insider UF-CMA if $Adv_A^{in-UF}(k)$ is negligible for every PPT adversary.

2.8.2 Identity-Based Signcryption

ID-based signcryption is mainly composed of four algorithms setup, extraction, signcrypt and unsigncrypt. Given a sender A and receiver B with identities u_a and u_b respectively, the scheme works as explained below (Dharminder & Mishra, 2020):

Setup: At first, the PKG inputs an appropriate security parameter (k), then generates corresponding public parameters $params$. The PKG publishes the parameters while keeping master-key secret.

Extraction: A user sends his own identity and requests the corresponding private key. Furthers PKG executes extraction algorithm using his master-key and computes a private-key d_i corresponding to the identity u_i.

Signcrypt: A runs algorithm Signcrypt($params, m, d_a, u_b) = \sigma$ *then* sends the output σ to the receiver.

Unsigncrypt: When the receiver B gets σ, Bexecutes the algorithm Unsigncrypt($params, \sigma, d_b, u_a) = m$ to recover the corresponding message. In 2003, (Boneh & Franklin, 2003) formalized the ID-Based cryptography by proposing an ID-based encryption scheme that was proven to be secure against Chosen Cipher Attack in the random oracle model (Dutta et al., 2004).

2.8.3 Certificateless Signcryption

A certificateless signcryption scheme consist of six algorithms: Setup, Set-Public key, Partial Private Key Extract, Set Private Key, Signcryption and Un-signcryption algorithms. The description of each probabilistic polynomial time algorithm is as follows:

i. *Setup(1^k):* The algorithm is run by KGC with security parameter k to output master secret key s and system parameters $params$.

ii. *Set-Public Key*: On input of user's secret-value$x_i$and system parameter$params$the algorithm returns users public key P_i

iii. *Partial Private Key Extract:* On input of user identity ID_i, user public keyP_i , master secret key s and KGC public key the algorithm computes d_i as partial private key then delivers d_i to the user.

iv. *Set Private Key*: This algorithm accepts input of system parameter $params$, user's partial private key d_i and secret value x_i. The algorithm returns user's full secret key SK_i.

v. *CLSC Signcryption*: This algorithm takes the private key of sender, message m_i, the identity of both sender $ID_s$and receiver $ID_r$and their respective public keys P_i to compute ciphertext σ

vi. *CLSC Unsigncryption*: On input of ciphertext σ, system parameter $params$ and receivers secret key x_r .The un-signcryption algorithm returns a message m_i or a symbol ⊥ for invalid.

A consistency requirement is defined as:

$\sigma \leftarrow Signcryption(params, m)$

$then$

$m \leftarrow Unsigncryption(params, \sigma)$

According to (Barbosa & Farshim,, 2008) in CLSC it is worth considering confidentiality and unforgeability in the IND-CCA-1 / IND-CCA-II and UF-CMA-I/UF-CMA-II under the following types of attackers.

Definition 2.8.3.1 (Type 1 Adversary): This models an adversary who is not in possession of the KGC's secret key. The adversary is denoted as A_I. This adversary is not permitted to extract the partial secret key for $ID_r \ or \ ID_s$ if the public key of this identity has been replaced before the challenge cipher was issued.

Definition 2.8.3.2 (Type II Adversary): This scenario models a curious KGC against which it is important to preserve confidentiality. The attackers can generate partial private key without running the partial secret key extraction oracle since he has the knowledge of msk. The adversary is not allowed to replace the public key for $ID_r \ or \ ID_s$ before the start of challenge.

The security is modeled through a game between the challenger and the adversary with regards to the two types of attacker IND-CCA2-I and IND-CCA2-II for purpose of confidentiality. Let the adversary of both types are denoted by A_I and A_{II}respectively. In the game the adversaries will interact with the Challenger denoted as C and keep a record of responses to queirs.

According to (Shoup, 2004) when proofing security using the sequence of games approach one needs to constructs a sequence of games, Game 0, Game 1,..., Game n, where the original attack game is Game 0 with respect to a give attacker and cryptographic primitive. It is desirable that the changes between successive games are very small as possible to ensure analysis of change is as simple as possible.

2.9 Related Work

In order to meet security needs of sensor nodes on resource constrained environments, lightweight cryptographic algorithm designed well is the key to constructing a riskless WSN scheme. (Zhong et al., 2016) propose an improved elliptic curve cryptography digital signature scheme for use on WSNs by optimizing the signature generation module of ECDSA, however they were unable to reduce the number of point additions and multiplication in the verification algorithm. (Zhang et al., 2011) developed a variant of ECDSA. (Sarath et al., 2014) found their scheme's signature generation and validation phase more complex and time consuming.

In 1997, (Zheng, 1997) introduced the concept of signcryption, he developed a signcryption scheme that was based on ElGamal cryptosystem that logically combined the functionality of digital signature and encryption. The scheme managed to reduce the cost of computation up to 50 % and the cost of communication up to 85 % compared to the tradition schemes which applied Signature-then-Encryption. The scheme requires complex interactive zero-knowledge proof to validate the non-repudiation and has no forward secrecy of message confidentiality (Nguyen et al., 2015; Ashraf et al., 2014) proposed a signcryption scheme based on ECC with lower computational cost which was later evaluated by (Toorani & Baheshti, 2009) who proved that it involves several security flaws, the scheme has weak session key establishment. (Singh & Vaisla, 2014) proposed a lightweight signcryption scheme based on ECC although they proofed that the scheme provided most of security goals including public verifiability it requires use of PKI for certificate management making it not suitable for WSNs.

Securing data in WBANs means that data cannot be accessed or altered by unauthorized persons. The security framework for a WBAN should support authorization, authentication and accountability for effective control of user access. This makes access control an important element for successful adoption of WBAN services (Chatterjee et al., 2013). However, effective implementation of an access control scheme in WBANs has been cited as a major problem (Shen et al., 2018). Zhou et al. (Zhou & Huang, 2010) proposed a constant size ciphertext policy from Attribute-Based Encryption (ABE) where size is not sensitive to the number of attributes in access control policies. However, Ali et al (Ali et al., 2020) found their scheme provided only a threshold access control policy and did not provide a flexible access structure. Ali et al. (Ali et al., 2020) went on to propose a lightweight fine-grained access control scheme for a WBAN. They put forward an ABE scheme based on lightweight encryption and decryption mechanism. To achieve a more secure data communication in WBANs environment, Hu et al. (2016) proposed an access control scheme that was based on Attribute Based Encryption and a digital signature. Their scheme was able to achieves a role-based access control by employing an access control tree. An access control that is context-aware bundled with a feature of anonymous authentication and a Hybrid CLSC scheme was proposed by (Arfaoui et al., 2019). Their security scheme exploits a transformation between and Attribute Based signcryption and an ID-based signcryption scheme in order to provide an adaptive privacy while meeting the security requirements. In 2013 (Hu et al., 2013) proposed an efficient approach to secure extra-body communication in WBANs. The approaches used in (Zhou & Huang, 2010; Ali et al., 2020; Arfaoui et al., 2019 and Hu et al., 2013) are based on ABE. However, the ABE requires costly cryptographic operations (Li & Hong, 2016) and is not suitable for use on resource constrained environments such as sensor networks (Li et al., 2010).

To prevent adversaries from exploiting WBAN services, (Narwal & Mohapatra, 2020) designed a mutual authentication and key agreement scheme for a two-tier WBAN that was energy efficient. In 2014, (Ma et al., 2014) used a signcryption scheme to construct an access control scheme for sensor networks. Their security scheme was based on the traditional public key infrastructure concept. However, the use of public key infrastructure has a serious problem of certificate management and therefore not suitable for use on resource constrained devices (Luo et al., 2018).

A lightweight Identity (ID) based encryption scheme for WBANs was designed by (Tan et al., 2009). Their approach was to allowed sensors to independently generate their public keys on-the-fly using an arbitrary string. In 2020 (Ramadan et al., 2020) gave a secure and efficient ID-based encryption scheme based on the RSA assumption while (Cagalaban & Kim, 2011) proposed an efficient access control scheme for use on WBAN. In their approach an ID-based signcryption was used to resolve data authentication problem. It has the advantage of chosen ciphertext security and enables group members to be stateless receivers in their communications. In 2020, (Shuai et al., 2020) discussed an authentication method for WBAN that was based on ID-based cryptography. Their approach eliminated online third-party participation and was suitable for multi-server architecture. ID-based schemes have an inherent key escrow problem and are not suitable for resource constrained devices since they present an element of vulnerability (Li et al., 2018).

A survey on WBANs was put forward by (Abidi et al., 2020) where they showed the importance of availability, authentication, confidentiality and integrity when implementing a secure WBAN. The use of certificateless signcryption in the design of an access control schemes provides the ability efficiently satisfy authentication, confidentiality, integrity, availability and non-repudiation with lower computation and energy cost (Li et al., 2016; Li et al., 2018). In 2016, (Li & Hong, 2016) proposed an access control scheme that was able to achieve user anonymity, confidentiality, authenticity, integrity and non-repudiation (hereafter called LH). They improved a signcryption scheme earlier proposed by (Barreto et al., 2008) and used it in the design of their access control scheme to achieve ciphertext authenticity and public verifiability. In 2014, (Liu et al., 2014) proposed an access control scheme using certificateless signature scheme for WBANs, their scheme was able to achieve user anonymity. (Sukanya et al., 2017) also improved the scheme by (Barreto et al., 2008) and proposed a trustworthy access control scheme for use on WBANs that was able to provide non-repudiation, confidentiality, authenticity, integrity and ciphertext authenticity. In 2016, (Li et al., 2016) also gave a certificateless signcryption scheme by modifying the scheme by (Barreto et al., 2008). They used the modified scheme in the design of a secure access control scheme that was able to satisfy ciphertext authenticity and public verifiability.

A novel CLSC scheme was proposed by (Li et al., 2018) in 2018. They proofed the security of their CLSC scheme in the random oracle model (ROM) and later used the scheme to design an anonymous and cost-effective access control scheme for the WBANs (hereafter called LHJ). Their proposed access control scheme was able to achieve confidentiality, integrity, authentication, anonymity and nonrepudiation. However, the schemes by (Li et al., 2018; Li & Hong, 2016; Sukanya et al., 2017) makes use of bilinear pairing cryptography. The computational cost of a pairing operation is complex and can be a burden when implemented on wireless sensor nodes (Gao et al., 2019). The major concern in WBANs is cost minimization and energy minimization when implementing access control schemes (Pawar & Kalbande, 2019). WBANs are not capable of performing energy-intensive and complex cryptographic operations, hence the need to develop solutions that will reduce energy consumption and communication overheads (Zou, et al., 2017). To overcome the challenges posed by use of pairing cryptography on resource constrained environments and the problem of key escrow, In 2019, (Gao et al.,2019) designed an access control scheme based on a certificateless signcryption scheme for use on WBANs (hereafter denoted as GPJ).

2.10 Research Gap

Wireless sensor networks have attracted a lot attention in recent years. They consist of autonomous sensor nodes. The sensors are portable and they have the capacity to sense, process and communicate data making them ideal for use in numerous application areas.

One major limitation of a Wireless Sensor Network is that they are resource constrained in terms of storage capacity, energy consumption, communication range and computational capability. This limitation is a critical factor to consider when implementing security protocols on WSNs.

Traditional security solutions often come with expensive cryptographic operations that consume rapidly the power available on resource constrained devices such as sensors leading to reduced life-time dedicated to applications (Singha et al., 2022). Elliptic curve cryptography has been proposed as efficient for use on resource constrained environments. However, the standard digital signature scheme known as ECDSA that falls under ECC has been cited as inefficient in computation. There is a need to improve the verification process of the ECDSA. Several researchers have proposed different variants of the digital signature scheme. However, the schemes proposed are still too complex in computations or insecure (Shim, 2017).

Signcryption provides us with an efficient approach to both signing and encrypting data and several signcryption schemes exist that make use of PKI or ID-based (Boneh & Franklin, 2003; Huang & Yang, 2017). The literature review in this thesis has discussed limitations of those schemes and shown that it is more efficient to develop schemes that are not dependent on PKI or ID-based concepts and the benefit of using certificateless cryptography.

Though certificateless cryptography affords an opportunity to develop efficient and secure schemes, most certificateless signcryption schemes are not optimized for use on WSNs. Most of their construction leads to complex computation and lack of ciphertext authenticity (Li et al., 2018) or they do not address all the basic security goals (Costa et al., 2017; Wahid & Mambo, 2016; Won et al., 2015). This thesis proposed a more lightweight and secure certificateless signcryption that addresses basic security goals and ciphertext authenticity for WSNs.

CHAPTER THREE

THE METHODOLOGY

3.1 Research design

The design of the study was quantitative. Experiments were conducted to generate data for the purpose of evaluating the performance of the proposed cryptographic schemes against other related schemes.

The research used theoretical and simulation empirical techniques to evaluate the performance of the proposed cryptographic primitives. The theoretical technique was used to identify the gaps in the existing literature on digital signature and signcryption schemes. The empirical technique was used to design or model related existing cryptographic primitives and the proposed cryptographic primitives through simulation experimental technique.

3.2 How the Research Objectives have been achieved

The first objective was to determine the techniques that can be used to adopt traditional digital signature primitives for use on WSNs. The aim was to identify the best techniques to adopt in this research. The research looked at comprehensive literature on cryptographic schemes and their construction. This led to the discovery of different techniques that have been used to adopt cryptographic schemes for use in resource constrained devices. The strengths and weaknesses of each method were identified and the best technique was determined and adopted.

The second objective was to design an efficient digital signature scheme, a variant of the ECDSA. Through a study of the original ECDSA, the strengths and weaknesses of the ECDSA were identified and a new variant of the ECDSA was designed as shown in section 4.2.2. Through experiments the performance of the proposed digital signature scheme was compared with the ECDSA as discussed in section 4.2.4.

The third objective was to use the proposed signature scheme in the design of a certificateless signcryption scheme. A comprehensive study on related literature review was undertaken to highlight how best to construct an efficient and secure signcryption scheme. The research did a cryptanalysis of the scheme by (Wei & Ma,2019) from where an efficient certificateless signcryption scheme was constructed as discussed in section 4.4.5. A certificateless pairing free signcryption scheme based on the proposed digital signature scheme was also constructed as discussed in section 4.5.2.

The fourth objective was to test the efficiency and security of the proposed schemes. The performance was tested in terms of efficiency in computational time, energy consumption and communication overhead. The performance of the proposed digital signature scheme was tested as discussed in section 4.2.4. ROM was adopted as a suitable approach in proving the security of the proposed signcryption schemes as discussed in section 4.5.3 and 4.6.1. The performance of the signcryption schemes against other related schemes is discussed in section 4.4.7 and 4.5.5.

3.3 Testing

The following operations contribute to the computation cost of a cryptographic scheme: The number of 1) elliptic curve point multiplication operation,2) elliptic curve point addition operation, 3) modular exponentiation operation, 4) modular inverse operation, 5) modular multiplication operation, 6) modular addition operation and 7) one-way or keyed one-way hash function (Singh & Vaisla, 2014). The hash function and Encrypt/Decrypt of symmetric crypto are negligible in both the proposed digital signature and the signcryption schemes.

3.3.1 Simulation software and tools

The simulation software and tools were used in this research as an alternative way of implementing and testing new concepts. They provided an avenue to perform repetitive performance analysis evaluations of the proposed cryptographic schemes. Cooja simulator was used to emulate wireless sensor nodes. Cooja simulator is supported by the Contiki operating system (Dunkels et al., 2004). Contiki is an operating system developed for networked environments. It is designed to support hardware devices that are severely constrained in terms of processing power, communication bandwidth and memory. The operating system comes with a sensor simulator called Cooja that is used to simulate sensor nodes. A typical Contiki system has communication bandwidth in the range of hundreds of kilobits/second, memory and processing speed measured in the order of kilobytes and mega Hertz respectively.

3.3.2 Performance Analysis

The performance analysis of the proposed digital signature scheme and signcryption schemes was evaluated as explained below:

3.3.2.1 Digital Signature Scheme

The proposed scheme was simulated on a MICAz mote. A MICAz mote is based on the low-power 8-bit microcontroller ATmega128L with a clock frequency of 7.37 or 8 MHz and was run on Contiki operating system. The Securities Exchanges Guarantee Corporation (SEC2, 2000) proposed recommended curves and domain parameters in (Brown D. L., 2010). The experiment was conducted for both the signature generation and verification process over prime field curves secp128r1, secp192r1, secp256r1 and secp384r1. The impact of the message size on the execution time was found to be negligible. The research compared the time taken by ECDSA and the proposed digital signature scheme in signing and verifying signatures in each round. Further, the scheme was used to design a broadcast multi-user authentication scheme for WSN and a certificateless pairing-free authentication scheme for WBAN whose performance was tested against other related schemes by (Omala et al., 2017) and (Izza et al., 2018). The tests were based on an approach adopted from (Liu et al., 2014) for the purpose of making the research work reproducible.

Computational analysis

The proposed schemes were evaluated in terms of computation cost against other related schemes. This research considered expensive Elliptic Curve operations: point multiplication, point addition, pairing operations and modular inverse operations used in the construction of the proposed schemes and other related schemes. The research looked at how many operations were used to generate a ciphertext or signature and how many operations were used to achieve verification or unsigncryption. Each Elliptic Curve operation was evaluated based on running time and energy consumption.

Communication efficiency

In the communication analysis this research looks at the communication cost involved in transmission of data in terms of total length of data transmitted which has an effect on energy cost. The proposed schemes were compared with other related pairing-free schemes based on ECC. The simulation considered a MICAz mote (Ali et al., 2011) which has a clock speed of 8 MHz with a 8-bit processor ATmega128L and a data rate of 12.4 kbps. The operating system used was the TinyOS where the power level of the MICAz sensor is given as 3.0 V. The current draw in active mode is 8.0 mA, receiving current draw is 10 mA and the sending current draw is 27 mA (Cao et al., 2008; Wander et al., 2005).

Energy cost

In the evaluation of the energy consumption of the proposed scheme against other related schemes, the research primarily considered scalar multiplication of the elliptic curve cryptography. Other ECC operations are ignored as they are negligible (Shim, 2007). The impact of communication cost on energy consumption for received and transmitted a message of n bytes are $W_r = V \times I_r \times n \times 8/r$ and $W_t = V \times I_t \times n \times 8/r$ respectively. The voltage is denoted as V while I_r denotes the current draw for receiving, I_t is the current draw for transmitting and r denotes the data rate. When a wireless sensor node adopts a flooding method to broadcast a message. The Wireless Sensor Network will only transmit its message once and will receive message N times, where N represents neighboring sensor nodes.

3.3.2.2 Signcryption Scheme

The efficiency of the proposed signcryption schemes was evaluated in comparison with other related schemes in terms of energy consumption, communication overhead and computational cost on a MICA2 mote as discussed in section 4.5.5. In computational cost only a point multiplication in G_1, pairing operation and exponentiation in G_2 are considered. Arithmetic operations and hash function were not considered since they do not have high computational cost (Cui et al., 2007). The power consumption on MICA2 is computed as $W = V * I * T$ where W denotes power in millijoules, voltage is represented by V, the current draw is denoted by I in milliamps $(mA)$and T denotes time in milliseconds(ms).

3.4 Security Analysis

The research looks at security from the perspective of Type-I and Type-II. Type-I adversary does not have access to the secret master key and is considered as an outsider. A Type-II adversary is considered as an insider adversary who has access to the master secret key.

There are two ways to proofing confidentiality security in chosen ciphertext attack (CCA). (1) The CCA-I notion can be adopted where an adversary is given access to a decryption oracle before receiving the challenge ciphertext or (2) The research can adopt CCA-II where the adversary has access to the decryption algorithm before and after receiving the challenge ciphertext. The CCA-II is a stronger and an adaptive notion. In this research confidentiality security of the proposed signcryption schemes was tested through the Random Oracle Model (Koblitz & Menezes, 2015) and they were proved secure in CCA-II notion. The unforgeability property of the proposed schemes was tested in existential unforgeability under Chosen Message Attack (EUF-CMA). A signcryption scheme is said to be EUF-CMA secure if no polynomial probabilistic time bound adversary Typer-1 and Type-II denoted as A_I and A_{II} respectively that can win the ROM game with a non-negligible advantage.

CHAPTER FOUR

RESEARCH RESULTS AND DISCUSSIONS

4.1 Introduction

This chapter provides the results of this thesis in terms of the proposed schemes. It covers the performance evaluation of the proposed digital signature scheme and signcryption scheme compared to other related schemes. Further, it provides the foundation and security analysis of the proposed signcryption scheme and a discussion of an application scenario.

4.2 A certificateless pairing-free Authentication protocol for WBAN

4.2.1 Introduction

In this chapter, A digital signature scheme that is a variant of the original ECDSA and apply the scheme in the design of an authentication scheme for WBAN (Kasyoka et al., 2020) is presented. Further, an analysis of the performance of the proposed scheme in comparison with other related schemes is given.

4.2.2 Proposed Digital Signature Scheme

This research has proposed an elliptic curve digital signature scheme that is more efficient in signing and verification process compared to the original ECDSA. The proposed scheme has reduced number of elliptic curve operations in both the signature generation and the verification process. One of the goals of this research was to improve computational efficiency in the signing and verification process making the scheme adaptable for use on resource constrained environments such as WSNs while still ensuring the security of the scheme.

4.2.2.1 Key Generation

In the key generation phase each signer must generate a pair of keys, one private and one public. The signer, let us call him Bob, generates the two keys using the following steps where G is a cyclic group of $E(F_q)$ generated by point P, with prime order n and identity $O, H: \rightarrow \{0,1\}, Z^n$ collision resistant hash function.

1. Select a random integer d, d $[1, n-1]$
2. Compute $Q = dP$.This is a point in the elliptic curve, Bobs public key is Q and private key is d. At this point $z = d^{-1}$ precompute and from the private key d.

4.2.2.2 Signing and Verification

Algorithm 3 - Digital Signature Generation

```
Step 1. Select integer $k, k \in_R [1, n-1]$
Step 2. Compute $R = k \cdot P$
Step 3. Compute $e = H(m)$
Step 4. Compute $s = z \cdot (e \cdot k) mod\ n$
Send pair is $(R, s)$and message $m$
```

Algorithm 4 - Digital Signature Verification

```
Step 1. Verify that s are integers in $[1, n-1]$
Step 2. Compute $e \leftarrow H(m)$
Step 3. Compute $w \leftarrow s \cdot e^{-1}\ mod\ n$
Step 4. Compute $X \leftarrow w \cdot Q$;
Step 5.  If $X = R$ accept signature else reject.
```

4.2.2.3 Digital Signature Correctness

The correctness of the proposed scheme is as follows:

$$X = k \cdot G$$

$$sdG = ekG$$

$$s \cdot Q = ekG$$

$$= (e^{-1}\ s)Q$$

4.2.3 Security Analysis

i. **Message Integrity Threats:** Should an active adversary make changes to the original message; the message will be rejected during the verification process as $H\ (m')^{-1} \neq H\ (m)^{-1}$that is required to recover value w.

ii. **Total Break**: If an attacker obtained message m and (R,s) and wants to obtain the private key d by he will first have to solve $z\ =\ (H\ (m) * k)/s$ to get the inverse of d, k is randomly selected ephemeral integer and so this will not be possible.

iii. **Signature Malleability**: In signature malleability from a given message signature pair, one can be able to derive a second signature of the same message. The standard ECDSA is not secure against signature malleability. Given $kP\ =\ (x_1, y_1)$ it makes use of information about x_1 , $x_1\ mod\ n$ but not the $y_1$which would imply $f(R) = f(-R)$and a message m can have two signatures, that is (m, r, s) and $(m, r, -s)$as explained by (Pointchevel et al., 2002) where any point with similar $(x_1,*)$ can be used to derive the second signature. Signature malleability is not possible in the proposed scheme as the full point $f(R)$ with exact (x_1, y_1) will be require for signature to be accepted.

4.2.4 Performance Analysis

4.2.4.1 Experimental Tool and Platform

The experiment was implemented on Contiki 2.7 (Dunkels et al., 2004) which is an open source operating system for the Internet of Things that connects tiny low-cost, low-power microcontrollers to the Internet. It runs on tiny microcontrollers and allows us to develop resource efficient applications while providing low-power wireless communication applicable on a range of hardware platforms. Contiki comes equipped with Cooja which is a tool that allows developers to test their code and systems on a simulator before they can run it on the target hardware.

The proposed scheme was simulated using the same characteristics of the sensor MICAz. The MICAz mote operates within the 2.4 GHz ISM band and is compliant with IEEE

802.15.4. It is based on the low-power 8-bit microcontroller ATmega128L with a clock frequency of 7.37 MHz and was run on Contiki operating system (Dunkels et al., 2004). The Securities Exchanges Guarantee Corporation (SEGC) proposed recommended curves and domain parameters in (Brown, 2010).

4.2.4.2 Cost Analysis

Given that the cost of an Elliptic Curve initialization is E. The time consumption of $plus/subtract$ operation is denoted as E1, $multiply$ operation E2, $modular\ arithmetic$ operation E3, $Hash$ operation E4 and E5 for modular inverse. The cost comparison of the proposed scheme against the original ECDSA is shown in Table 3.

Table 3: Cost Comparison

Scheme	Operation	Cost Comparison
ECDSA	Generation	E+n(E1+3E2+2E3+E4+E5)
	Verification	E+n(E1+4E2+2E3+E4+E5)
Ours	Generation	E+n(3 E2+E3+E4+E5)
	Verification	E+n(2E2+E3+E4+E5)

4.2.4.3 Computational Efficiency

In the signature generation and verification process test was conducted for each curve using a similar approach as used in (Nguyen et al.,2015). The impact of the message size on the execution time was found to be negligible. This research compared the time taken by ECDSA and the proposed scheme to sign and verify signatures in each test. Test was performed on efficiency in terms of computation time where time was measured in milliseconds. The proposed digital signature scheme was able to achieve a 11% marginal improvement in signing process which can be attributed to the precomputation of d^{-1} in the signing process and a 19.3% improvement in the signature verification process which can be attributed to the reduction in the number of elliptic curve operations in the verification process. Experimental results for the signing process, verification process and average time taken to verify in secp128r1, secp192r1, secp256r1 and secp384r1 are shown in Figure 4 and Figure 5, Table 4 and Table 5 respectively.

Table 4: Average Signature Generation Time

	Sample 1	**Sample 2**	**Sample 3**	**Sample 4**
	secp128r1	secp192r1	Secp256r1	Secp384r1
ECDSA	1.56	4.4	10.05	30
Proposed Scheme	1.4	3.52	9	27
Difference in seconds	0.16	0.88	1.05	3

Table 5: Average Signature Verification Time

	Sample 1	**Sample 2**	**Sample 3**	**Sample 4**
	secp128r1	secp192r1	Secp256r1	Secp384r1
ECDSA	1.95	4.6	13.2	32.45
Proposed Scheme	1.5	3.5	9.0	27.4
Difference In seconds	0.45	1.1	4.2	5.05

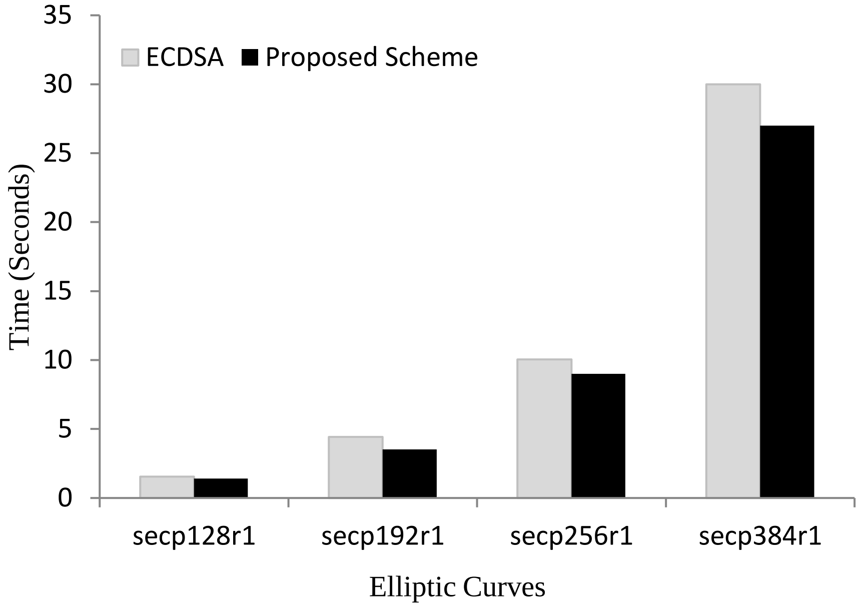


Figure 4: Signature Generation Time

.

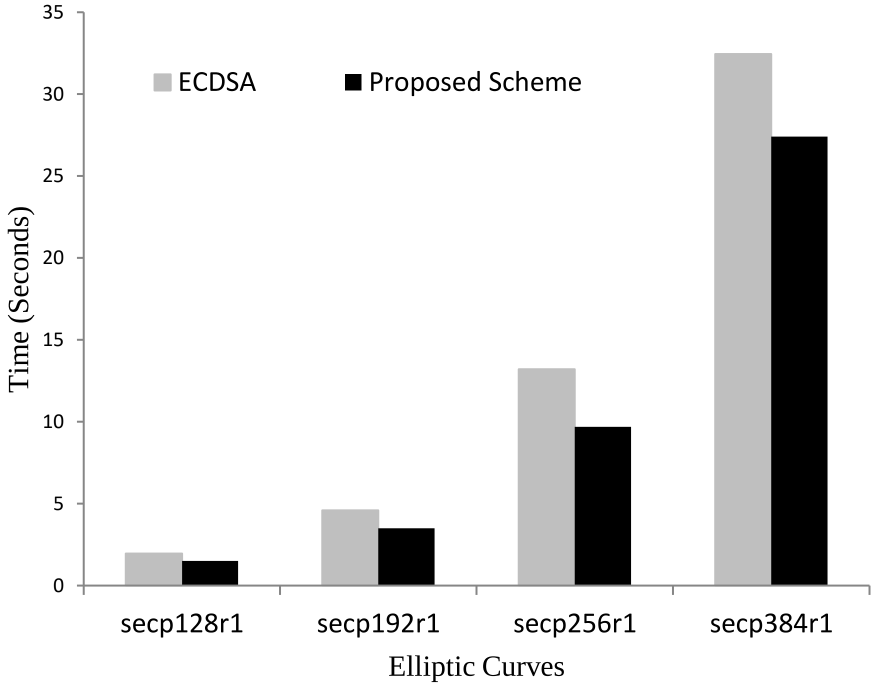


Figure 5: Signature Verification Time

4.2.5 Application Area

A WBAN is based on a wireless sensor network (Jian et., 2016) and comprises of a data sink, a Trusted Authority (TA) and an interconnection of multiple sensors (Anusya et al., 2018). Through a minor surgery the sensor nodes used in WBANs can be surgically implanted inside a patient's body or they can be attached surface of a patient's body. In other circumstances they can also be used as external nodes that do not have contact with the patient's body (Khalilian et al., 2016). Figure 6. Shows the network model of the proposed authentication scheme.

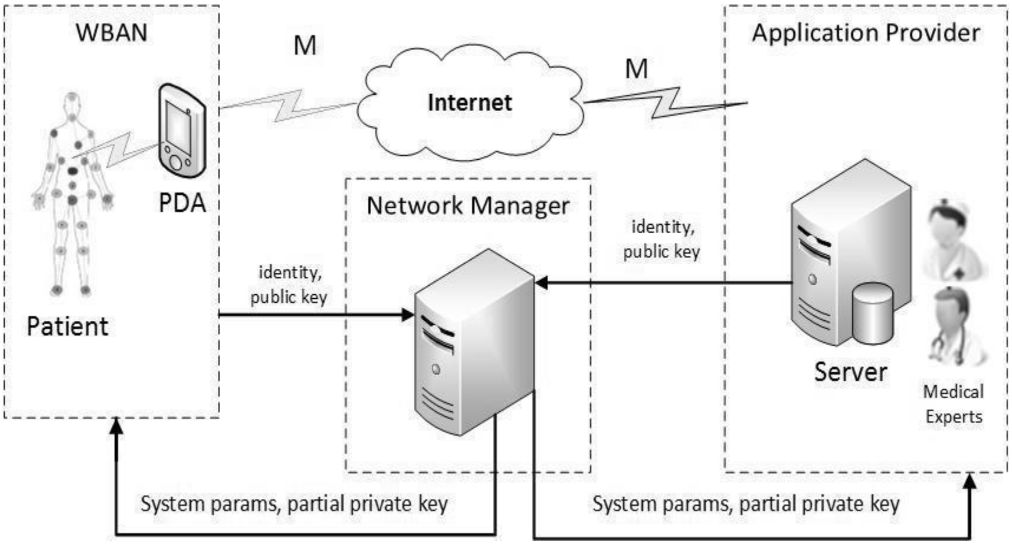


Figure 6: Network Model

4.2.5.1 Proposed Authentication Scheme for WBAN

In this sub section, an authentication scheme that is based on the proposed digital signature scheme is presented. Table 6 show the system notation used in the proposed authentication scheme. The authentication scheme is made up of three phases:

- *Initialization*: In this phase, the Network Manager has the task of selecting the cryptographic hash functions, the system parameters and sets its secret and public key. NM publishes the system parameters, hash functions and the public key.
- *Registration:* In the registration phase a PDA or a smartphone acts as the client denoted as C and is used to control all the sensor nodes in WBAN. Both the Application Provider denoted as AP and the client C set their private and public keys then register their details with the NM.
- *Authentication*: In this phase, before C can be allowed to transmit patient's physiological data both the client C and AP authenticate each other.

Table 6: Notation of Symbols

Notation	Description
P_{pub}	Public Key for Network Manager
NM	Network Manager
C	WBAN Client
AP	Application Provider
x_C	Private Key for Client
x_{AP}	Private Key for Application Provider
PK_C	Public Key for Client
PK_{AP}	Public Key for Application Provider
sk	Session Key
tt_i	Timestamp
$H(\cdot)$	One-way function
M_i	Message
v	Signature

Initialization

The Network Manager denoted as NM who acts as a KGC,will be required to select an elliptic curve $E(F_q)$ over finite field F_q where the $E(F_q)$ is defined by the chosen system parameters. NM chooses randomly a master secret key msk where $msk \in_R Z_q^*$ and computes its general public key$P_{pub} = msk \cdot P$ and defines secure cryptographic hash functions:$H_0: \{0,1\}^l \times G_1 \rightarrow Z_q^*$, $H_1: G_1 \rightarrow Z_q^*$, $H_2: G_1^2 \times \{0,1\}^{2l} \rightarrow Z_q^*$, $H_3: \{0,1\}^l \times Z_q^* \rightarrow Z_q^*$, $H_4: G_1 \times Z_q^* \rightarrow Z_q^*$and $H_5: \{0,1\}^{4l} \times Z_q^* \rightarrow Z_q^*$. The Network Manager publishes the system $params$ as $\{P, G_1, P_{pub}, E(F_q), H_0, H_1, H_2, H_3, H_4, H_5\}$ where value l represents the length of an identity.

Registration

The registration process allows the WBAN client C and AP to register with the network manager NM.

AP Registration

1. An AP with identity $ID_{AP} \in_R \{0,1\}^l$ sends its identity to NM.
2. On receiving ID_{AP} , NM computes $pp_{AP} = msk. H_0(ID_{AP}, P_{pub}) mod\ q$ as the partial private key for AP and secretly sends pp_{AP} to AP.
3. When the AP receives pp_{AP} it verifies its validity by checking if equation $pp_{AP}P = Ppub. H_0(ID_{AP}, P_{pub})$ holds. If it holds, it will randomly choose a secret value $x_{AP} \in_R Z_q^*$ then set $sx_{AP} = pp_{AP} \cdot x_{AP}\ mod\ q$ as its secret key. The AP will compute $PK_{AP} = sx_{AP} \cdot P$ as its public key then proceed to set another secret value $t_{AP} = sx_{AP}^{-1}\ mod\ q$. The full private key will be set as $FK_{AP} = (pp_{AP}, sx_{AP}, t_{AP})$.

WBAN Registration

1. The WBAN with identity $ID_C \in_R \{0,1\}^l$ sends its identity to NM.
2. On receiving ID_C , NM computes $pp_C = msk. H_0(ID_C, P_{pub}) mod\ q$ as the partial private key for C and secretly sends the partial private key pp_C to client C.

3. When the C receives pp_C it verifies its validity by checking if equation $pp_CP = Ppub.H_0\left(ID_C, P_{pub}\right)$ holds. If it holds, it will randomly choose a secret value $x_C \in_R Z_q^*$ then set $sx_C = pp_C \cdot x_C \, mod \, q$ as its secret key. The AP will compute $PK_C = sx_C \cdot P$ as its public key then proceed to set another secret value $t_C = sx_C^{-1} \, mod \, q$. The full private key will be set as $FK_C = (pp_C, sx_C, t_C)$.
4. The client C will compute $PK_{AP}^* = sx_CPK_{AP} + h \cdot P_{pub}$ for the AP it intends to transmit data to. Note $h = H_0\left(ID_C, P_{pub}\right)$.

Authentication

There is a need for AP and C to authenticate each other before they can exchange physiological data. Figure 7 shows the authentication process of the proposed scheme. The authentication process is as follows:

1. Client C selects random integer $k \in_R Z_q^*$ and computes $n = k \cdot t_C$ then sets $\beta = H_1(k \cdot PK_{AP})$ and $c_0 = H_2(PK_{AP}^*, PK_C, ID_C, ID_{AP})$. The signature is computed as $v = (c_0 \cdot n) mod \, q$. C set $Auth_1 = H_3(\beta, v)$ and sends service request message $M_1 = \{v, Auth_1, tt_1\}$ to AP.
2. When AP receives message M_1 at time tt_2, it checks the validity of tt_1. AP will reject M_1 if $tt_2 - tt_1 \geq \Delta T$, given that ΔT is the valid transmission delay time. If tt_1 is fresh, AP will set $c_0 = H_2(PK_{AP}^*, PK_C, ID_C, ID_{AP})$ then compute $Q = (v \cdot c_0^{-1})sx_{AP} \cdot PK_C$ and sets $Auth_2 = H_3(H_1(Q), v)$. The AP will check if $Auth_1 = Auth_2$ holds, if it holds AP will compute $Auth_3 = H_4(sx_{AP} \cdot PK_C, v)$.The session key will be set by the AP as $sk = H_5(tt_1, tt_2, ID_C, ID_{AP}, Auth_3) \oplus H_1(Q)$, and responds to client C with the message $M_2 = \{Auth_3, tt_2\}$.
3. On receiving M_2 at time tt_3 client C will check if tt_2 is fresh, if it is not fresh message M_2 will be rejected else C will compute $Auth_4 = H_4(sx_C \cdot PK_{AP}, v)$. Client C will check if $Auth_3 = Auth_4$ and sets the shared session key as $sk = H_5(tt_1, tt_2, ID_C, ID_{AP}, Auth_4) \oplus \beta$.

Correctness of the Scheme

The authentication correctness of the proposed scheme is as follows:

$$Q = (v \cdot c_0^{-1}) sx_{AP} \cdot PK_C$$

$$= (c_0 \cdot n \cdot c_0^{-1})\ sx_{AP} \cdot PK_C$$

$$= (c_0 \cdot k \cdot t_C \cdot c_0^{-1}) sx_{AP} \cdot PK_C$$

$$= (k \cdot t_C) sx_{AP} \cdot sx_C P$$

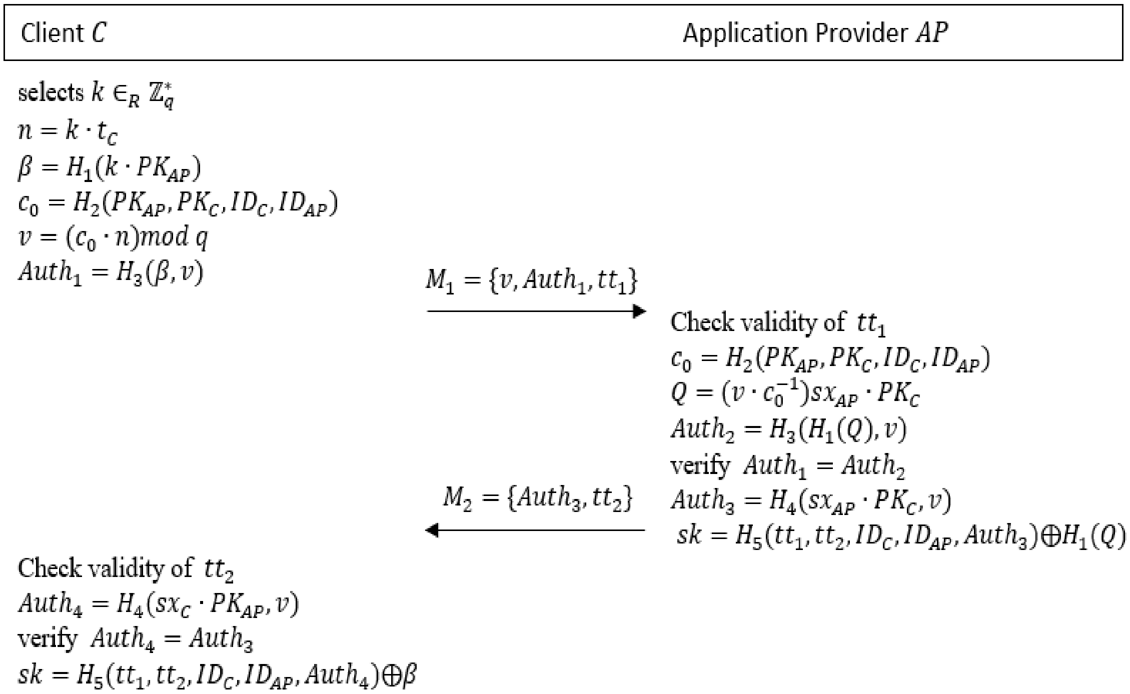
$$= k \cdot \frac{1}{sx_C} \cdot sx_{AP} \cdot sx_C P$$

$$= k \cdot sx_{AP} \cdot P$$

$$= k \cdot PK_{AP}; Then\ H_1(k \cdot PK_{AP}) \rightarrow \beta$$

While the correctness of the session agreement is as follows:

$$\begin{aligned} Auth_3 &= H_4(sx_{AP} \cdot PK_C, v) \\ &= H_4(sx_{AP} \cdot sx_C \cdot P, v) \\ &= H_4(sx_C \cdot PK_{AP}, v) \\ &= Auth_4 \end{aligned}$$



Client C Application Provider AP

selects $k \in_R \mathbb{Z}_q^*$

$n = k \cdot t_C$

$\beta = H_1(k \cdot PK_{AP})$

$c_0 = H_2(PK_{AP}, PK_C, ID_C, ID_{AP})$

$v = (c_0 \cdot n) mod\ q$

$Auth_1 = H_3(\beta, v)$

$M_1 = \{v, Auth_1, tt_1\}$

Check validity of tt_1

$c_0 = H_2(PK_{AP}, PK_C, ID_C, ID_{AP})$

$Q = (v \cdot c_0^{-1}) sx_{AP} \cdot PK_C$

$Auth_2 = H_3(H_1(Q), v)$

verify $Auth_1 = Auth_2$

$M_2 = \{Auth_3, tt_2\}$

$Auth_3 = H_4(sx_{AP} \cdot PK_C, v)$

$sk = H_5(tt_1, tt_2, ID_C, ID_{AP}, Auth_3) \oplus H_1(Q)$

Check validity of tt_2

$Auth_4 = H_4(sx_C \cdot PK_{AP}, v)$

verify $Auth_4 = Auth_3$

$sk = H_5(tt_1, tt_2, ID_C, ID_{AP}, Auth_4) \oplus \beta$

Figure 7: Authentication Process

4.2.5.2 Security Analysis of proposed Authentication scheme.

In this subsection, a pairing-free authentication scheme for WBAN can meet the security requirements proposed in subsection 2.2.6 is proposed.

Theorem 1 *The proposed scheme provides user anonymity*

Proof: The client sends value v computed as $v = (c_0.n) mod\ q$. The value c_0 contains the identity of the client and is encrypted in value v. The adversary will need to know value to recover c_0 , n is computed as $n = k \cdot t_C$ where k is a secret ephemeral value t_C is a secret value only known to the client. Therefore, proposed authentication system provides user anonymity.

Theorem 2 *The proposed scheme provides Mutual Authentication*

Proof: The attacker will need to solve $Auth_1$ computed as $Auth_1 = H_3(\beta, v)$. From theorem 1, the attacker will have to compute value n from two unknown values $k$and t_C and solve c_0. If the attacker succeeds in Theorem 1 then he will have to compute β by solving DLP to find the value k^* that satisfies the equation $\beta = H_1(k^* \cdot PK_{AP})$ for the attacker to output a valid value β^* that solves $Auth_1 = H_3(\beta^*, v)$ this will imply that only the client can be the originator of the message.

Theorem 3 *The proposed scheme provides forward secrecy.*

Proof: The proof starts with the assumption that an adversary has access to private keys of both the client C and application provider AP and has access to value v that was obtained from a past session. The adversary will not be able to compute and output a valid value v since it is computed using a random ephemeral key k . The value is known to the client C.

Theorem 4 *The scheme provides security against impersonation attack.*

Proof: If an adversary intends to impersonate C, then the adversary must provide the correct values for message $M_1 = \{v^*, Auth_1^*, tt_1\}$. AP will not be able to authenticate $Auth_1$ as computing $Q' = (v \cdot c_0^{-1})sx_{AP} \cdot PK_C$ and setting $Auth_2 = H_3(H_1(Q'), v^*)$ will not satsfy $Auth_2 = Auth_2$.

Theorem 5 *The proposed authentication scheme provides resilience to stolen verifier attack*

Proof: Given the fact that the proposed scheme does not maintain verification table, then the proposed scheme is secure against stolen verifier attack.

Theorem 6 *The proposed scheme provides unlinkability*

Proof: In the proposed scheme a valid session can only be linked to ID_C of C by the AP since the identity ID_C is encrypted in value v . The value v will always keep changing with every execution of the authentication algorithm.

Theorem 7 *The proposed scheme provides known-key security.*

If a past authentication session key sk is compromised, an attacker will have a negligible advantage in compromising future authentication session key. Every time the authentication algorithm is executed a unique sk will always be generated. The session key sk is composed of value $Auth_3$ that is generated using secret key sx_i and value v . Value v is unique with every authentication process executed. To recover sx_i an attacker with the knowledge of public key PK_i will need to solve Discreet Logarithm Problem (DLP) which is a hard problem.

4.2.5.3 Performance Analysis

The efficiency of the proposed authentication scheme with schemes by (Omala et al., 2017) and (Izza et al., 2018). In the analysis, an approach proposed by (Liu et al., 2014) is used where the running time of three cryptographic operations; EC scalar multiplication operation, bilinear pairing operation and Hash operation denoted as T_{SM} , T_P and T_H respectively is shown in Table 7.

Table 7: Cryptographic running time

	AP(ms)	WBAN C(ms)
T_{SM}	6.38	30.67
T_P	20.04	96.35
T_H	3.04	14.62

In 2017, to achieve a trusted security level (He et al., 2017) used super singular $E(F_p)$ with order q over finite field F_p where q and p represents two prime numbers with 160 and 512 bits respectively. The lengths of G_1 and G_2 are 1024 and 512 bits respectively while the lengths of identity and timestamp are 32bits each and the authentication message using message authentication code MAC is set as 1024 bits. The communication cost of the proposed authentication scheme is shown in Table 8. Compared to the scheme by (Omala et al., 2017), the communication efficiency of the proposed scheme is 77% and 84.2% in login and authentication respectively. The communication efficiency of the proposed scheme compared to the authentication scheme by (Izza et al.,2018) is 74% in login and 81% in the authentication phase. The running time of the proposed scheme compared to schemes by (Omala et al., 2017) and (Izza et al.,2018) is shown in Table 9.

As shown on Table 4, the proposed authentication scheme is 71.4% and 68.2% more efficient in AP and C computations respectively compared to the scheme by (Omala et al., 2017). The proposed scheme is computationally more efficient in C compared to the scheme by (Izza et al.,2018) by 68.2%. However, their scheme registered the same level of efficiency compared to the proposed scheme in AP. The results of the proposed scheme are more desirable considering the fact that C is resource constrained and $AP's$ servers are not resource constrained.

Table 8: Communication Cost Comparison

Scheme	Login	Authentication
Omala et al.,2017	$\lvert G_1 + T_1 + z * Z_q^* + ID \rvert$ $1024 + 32 * 2 + 2 * 160 \approx 1536\ bits$	$\lvert G_1 + T_2 + Z_q^* \rvert$ $1024 + 32 + 160 \approx 1216\ bits$
Izza et al.,2018	$\lvert Z_q^* + G_1 + Z_q^* + T_1 \rvert$ $160 + 1024 + 160 + 32 \approx 1376\ bits$	$\lvert MAC \rvert$ $\approx 1024\ bits$
Ours	$\lvert Z_q^* + Z_q^* + T_1 \rvert$ $160 + 160 + 32 \approx 352\ bits$	$\lvert Z_q^* + T_1 \rvert$ $160 + 32 \approx 192\ bits$

Table 9: Performance Analysis

Scheme	AP	WBAN
Omala et al.,2017	$7T_{SM} \approx 44.66$ ms	$3T_{SM} \approx 92.01\ ms$
Izza et al.,2018	$2T_{SM} \approx 12.76$ ms	$3T_{SM} \approx 92.01$ ms
Ours	$2T_{SM} \approx 12.76$ ms	$2T_{SM} \approx 29.24\ ms$

4.2.6 Summary

WBANs have proven to be of great importance in the medical healthcare practice. However, due to the resource constrained nature of WBAN, the implementation of their security can be a major challenge that needs to be resolved fast enough to avert a disaster in the society. In this thesis, an efficient pairing-free certificateless authentication scheme was proposed. The proposed authentication scheme was evaluated against other related authentication schemes and the results have shown that the proposed scheme is secure and more efficient in terms of communication cost and computational overhead. The efficiency of the proposed scheme makes it more suitable for use on resource constrained environments such as WBANs.

4.3 Multi-user Broadcast Authentication scheme for WSN based on Elliptic Curve Cryptography

4.3.1 Introduction

A slow signature verification process in a Broadcast Authentication (BA) scheme will lead to high energy consumption that can impact negatively the life span of a sensor node in a WSN. Broadcast authentication is an important feature in WSNs. Hence, it has become important for us to develop efficient and lightweight broadcast authentication. There is a need to guarantee basic security goals are achieved in a more efficient manner especially on resource constraint devices or environments.

Efficient authentication schemes based on symmetric cryptography do exist (Mansoor, et al., 2019; Ghani, et al., 2019). A sender and its receivers share the same secret key, there is a chance that one of the receivers can impersonate a sender and transmit forged messages to other receivers. This problem is inherent in all symmetric cryptographic schemes and to overcome the problem public key encryption is used (Chang et al., 2006). In public-key infrastructure (PKI) the users' public keys are bound to the respective users' identities by means of public-key certificates that are issued by a Certificate Authority (CA) (Shim, 2007). The signature of the Certificate Authority on the certificate is used for the purpose of preserving the authenticity of the public key of a corresponding user. The CA keeps a record of the identity of a user together with the user's own public key so they can be used later to verify the user's public key. The CA also performs certificate management activities such as certificate issuance, certificate renewal and certificate revocation (Subhas et al., 2019). Certificate management has been shown to lead to extra storage, large computation and communication costs (Gayathri et al., 2018).

The use of the original ECDSA is not appropriate for achieving mutual authentication between the entities like the sink, cluster heads and sensor nodes (Moon et al., 2016). Speeding up of ECDSA's signature generation process and verification process is a problem of great importance. To this end, this research proposes a new broadcast authentication scheme for WSN with message recovery that makes use of the proposed efficient elliptic curve digital signature scheme.

4.3.2 Proposed Signature Protocol

With a slight modification of the proposed variant of the ECDSA, this research proposed a signature protocol with message recovery property that consists of four phases: Setup, key generation, signature generation and signature verification.

4.3.2.1 Set Up

Given security parameter γ, an elliptic curve $E(F_p)$ is selected which is defined over finite field F_p where p represents number of points on the elliptic curve. G is a cyclic group of $E(F_p)$ that is generated by a generator point $P \in G$, with prime order q . Pick a random $msk \in Z_q^*$ and compute $P_{pub} = msp \cdot P$. Select a cryptographic hash functions $H_1\colon \{0,1\}^2 \rightarrow Z_q^*$ and $H_1\colon \{0,1\}^2 \times G \rightarrow Z_q^*$that are collision resistant. System parameters are set as $param < F_q, E, p, G, Q, P_{pub}, H_1, H_2 >$ and the master secret key is msk.

4.3.2.2 Key Generation

The key generation process will proceed as follows: Select a random integer $d \in_R Z_q^*$, given a user identity ID compute $v = msk + H_1(ID_i, d)$, Compute $Q = vP$ and $z = v^{-1} \, mod \, q$. Where Q is a signer's public key and full private key is set as $SK = (d, z)$.

4.3.2.3 Signature Generation

Select integer $k \in_R Z_q^*$;Compute $F = k \cdot P$; If F_x =0 then go to start else, compute $e = m \oplus d \parallel F_x$ where F_x denotes the x-coordinate of point $F = (x, y)$; $c = H_2(e, ID, P_{pub})$; $s = z \cdot (c \cdot k) mod\ q$ then sends signature as $\sigma =< F, s, e, c >$. The message m is not transmitted together with the signature generated as the proposed digital signature scheme has a property of message recovery.

4.3.2.4 Signature Verification

Upon receiving $\sigma =< F, s, e, c >$, the verification process proceeds as follows:

Check if equation $c = H_2(e, ID, P_{pub})$ holds, if it does not hold drop the message else compute $w = s \cdot e^{-1} mod\ q$; $X = w \cdot Q$. If $X = F$ then accept the signature received and recover the message by computing $m' = e \oplus d \parallel F_x$ else reject the signature.

Correctness The correctness of the proposed scheme is as shown below:

$$X = w.Q = s \cdot c^{-1}Q = z(c \cdot k)c^{-1}Q = z \cdot k \cdot Q = d^{-1} \cdot k \cdot Q = d^{-1} \cdot k \cdot dP$$
$$= k \cdot P = F$$

4.3.3 Broadcast Authentication Scheme

The proposed scheme is made up of four parts: (1) Initialization, where wireless sensor nodes are initialized by the sink; (2) Sensor addition, in which the sink generates a public/private key pair for the new sensor node joining the sensor network; (3) Broadcast authentication scheme, in which a wireless sensor signs a message and broadcasts it to the neighboring wireless sensors and eventually the message relied to the sink as depicted in Figure 8. (4) Sensor revocation process, which maintains a list of all the compromised sensor nodes.

4.3.3.1 Initialization

The BS playing the role of a KGC selects an elliptic curve E over finite field F_q and $P \in G$ of prime order q. BS defines a secure cryptographic hash functions$H_1: \{0,1\}^* \times G \times G \to Z_q^*$, $H_2: \{0,1\}^2 \to Z_q^*$, $H_3: \{0,1\}^2 \times G \to Z_q^*$ and $H_4: \{0,1\} \to Z_q^*$ then selects secret key $msk \in_R Z_q^*$ as its master secret key. The BS proceeds to compute its own master public key as $BS_{pk} = msk \cdot P$, and sets another secret value $z_b = msk^{-1}\ mod\ q$.

4.3.3.2 Key Generation

In this phase, the private keys and public keys for each sensor node will be generated by the base station. Given identity $WS_{ID_i} = H_4(ID)$ for a sensor node, the BS begins by selecting a random value $d_i \in_R Z_q^*$ proceed to compute $v_i = msk + H_1(WS_{ID_i}, d_i)$ then sets public key for a sensor as $Q_i = v_i P$. A random value $vt \in_R Z_q^*$ is selected and set as a common verification token for all sensor nodes in the network which can be changed regularly by the BS. The private key for a sensor node will be set as $SK = (d_i, z_i, vt)$ where$z_i = v^{-1}\ mod\ q$ and vt is a general verification token. To reduce the amount of communication overhead, all the sensor nodes before deployment to the WSN are pre-configured with sensors' information such as $BS_{pk} z_i$,d_i, a list of public keys and identities used by the sensor registered in the wireless network and the elliptic curve parameters. To ensure each sensor node device is protected from physical device capture, a user is allowed to select a secret password PW then use his/her PW to computes $d' = H_4(PW)^{-1}d$, $z' = H_4(PW)^{-1}z$ and $vt' = H_4(PW)^{-1}vt$. Following the approach proposed in (Cao et al., 2008), a user who wants to recover the private key will first have to enter a valid password PW to recover (d, z, vt) from the stored (d', z', vt').

4.3.3.3 Message Broadcast Authentication

To send an authenticated message to a base station in a WSN, a sensor with identity WS_{ID_i} will proceed as follows:

Algorithm 5: Signature Generation

```
1. Choose a random value $k \in_R Z_q^*$ and compute $F = k \cdot P$;
2. If $F_x = 0$ goto step 1;
3. Compute $e = m_i \oplus d_i \parallel F_x$ where $m_i$ is the message;
4. Compute $c = H_2(e, WS_{ID_i}, BS_{pk}, vt)$ and output $\sigma_i =< F, s, e, c >$ as the
   signature.
```

The sender will broadcast message $< \sigma_i, WS_{ID}, tt_i >$ to the next hop where s is generated using the signing algorithm of the proposed protocol and tt_i is the current timestamp of the sensor node signing the message. The proposed scheme has the property of message recovery whereby message m_i signed does not need to be forwarded together with the signature. It can be recovery in the verification process of the proposed broadcast authentication scheme. Message recovery technique will aid in minimizing communication overhead by reducing on size of message transmitted over the wireless network (Shim, 2007).

Messages will be signed once by the sender sensor node then forwarded to the BS by the intermediate nodes. The neighbouring sensor node will verify the transmitted message using the verification algorithm of the signing protocol and will forward to the next neighboring sensor. As the same message moves along the network, it will be verified a number of times by different sensor nodes until it reaches the designated BS. By reducing the cost of operations in the signature verification phase of the proposed signature protocol, the computational cost of each sensor node during the verification process will be reduced. This will be due to the reduction of computational cost. Hence, the overall energy consumption of the Wireless Sensor Network is significantly reduced.

4.3.3.4 Sensor Message Authentication

The authentication process for each sensor node before the message reaches the BS is conducted as follows: When the neighboring sensor node receives $< \sigma_i, WS_{ID}, tt_i >$ it checks iftt_i and WS_{ID} are valid else drops. It will check if equation $c = H_2(e, WS_{ID_i}, BS_{pk}, vt)$ holds, if it does not hold it will drop the message else it will forward massage $< \sigma_i, WS_{ID}, tt_i >$ to the sensor node in the next hop. A similar process of verification will continue until the message reaches the BS. In an environment where resources are constrained such as WSNs, speeding up the signature verification process is a problem of considerable practical importance (Benzaid et al., 2012). The approach used to validate c is ciphertext authenticity. It helps reduce the cost of computation of the neighboring nodes by ensuring that they do not have to run the entire signature verification process as prescribed in the proposed signature protocol.

4.3.3.5 Base Station Message Authentication

When BSreceives $< \sigma_i, WS_{ID}, tt_i >$ it checks for validity of the data as follows:

Algorithm 6: Signature Verification

1. BSchecks if tt_i is fresh as per set time delay threshold else it discards the data.
2. Checks if $WS_{ID}$is valid else drop data.
3. Run the proposed verification algorithm on the message received. If the verification process is successful it recovers the message m_i as $m_i{}' = e \oplus d_i \parallel F_x$.

4.3.3.6 Revocation

A sensor node whose message fails the verification process are immediately reported to the base station by the verifying sensor node where further investigations can be conducted. If the node is found to have been compromised by an adversary it will be added to the revocation list. The BS will generate a signature on message $m = \left(WS_{ID_x} || Rev\right)$, where Rev is a revocation message and WS_{ID_i} is the identity of the compromised wireless sensor node. It will selecting a value $k \in_R Z_q^*$and compute $F = k \cdot P$ then encrypts message m as $e = m \oplus vt || F_x$, $c = H_3\left(e, vt, BS_{pk}\right)$ and set the signature as $\sigma_i =< F, s, e, c >$. The base station will broadcast message $M_{Rev} =< \sigma_i, tt_i >$ to all sensor nodes in the network, where s is a signature generated using the signing algorithm of the proposed signature protocol and tt_i is the current timestamp of the BS. When a sensor receives the message M_{Rev} it runs the process outlined in the proposed verification algorithm to validate the message. If the verification process is successful, the sensor node recovers $m' = \left(WS_{ID_x} || Rev\right)$ and adds WS_{ID_x} to its own revocation list. If the wireless sensor receives a message from a sensor node whose identity is in revocation list it will immediately drop the message.

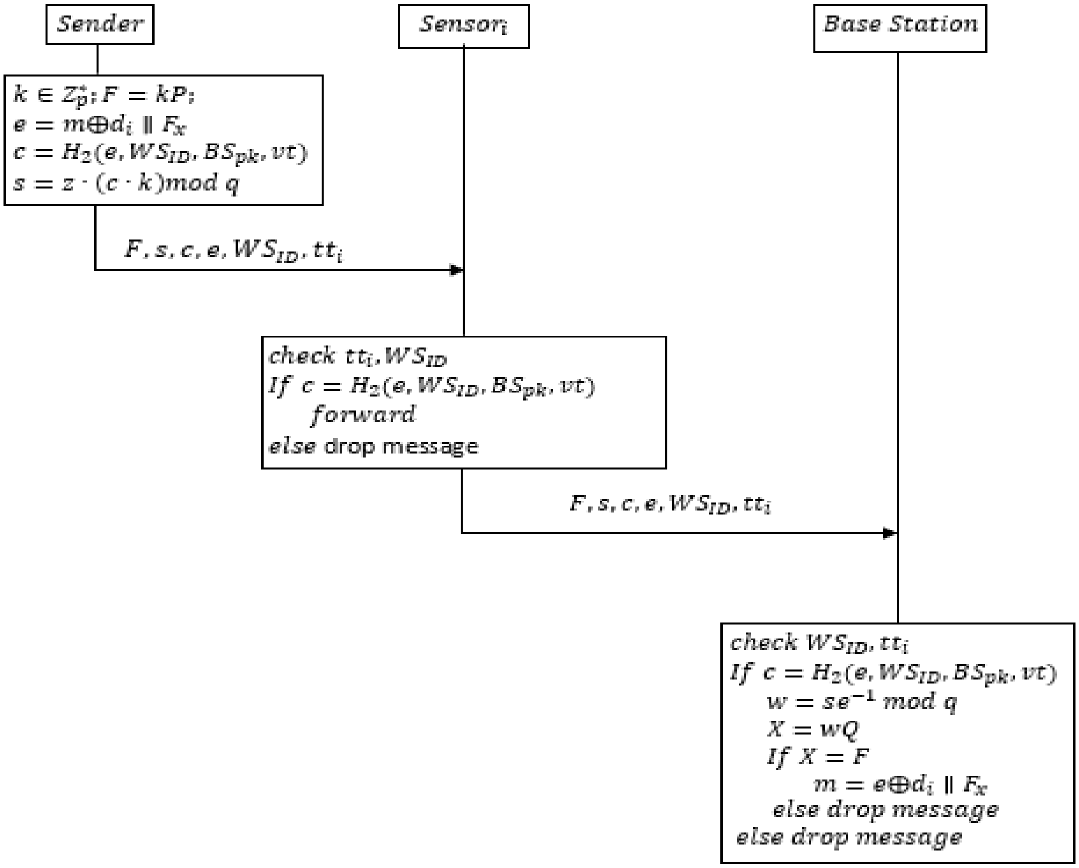

$Sender$
$Sensor_i$
$Base\ Station$
$k \in Z_p^*; F = kP;$
$e = m \oplus d_i \parallel F_x$
$c = H_2(e, WS_{ID}, BS_{pk}, vt)$
$s = z \cdot (c \cdot k) mod\ q$
$F, s, c, e, WS_{ID}, tt_i$
$check\ tt_i, WS_{ID}$
$If\ c = H_2(e, WS_{ID}, BS_{pk}, vt)$
$forward$
$else$ drop message
$F, s, c, e, WS_{ID}, tt_i$
$check\ WS_{ID}, tt_i$
$If\ c = H_2(e, WS_{ID}, BS_{pk}, vt)$
$w = se^{-1}\ mod\ q$
$X = wQ$
$If\ X = F$
$m = e \oplus d_i \parallel F_x$
$else\ drop\ message$
$else\ drop\ message$

Figure 8: Broadcast Authentication Scheme

4.3.4 Security Analysis

The proposed authentication scheme is secure against the following security properties:

a) *The proposed authentication scheme provides data confidentiality.* The messages forwarded from the WS_i to the the BS are encrypted into ciphertext c and signed any attacker trying to intercept the communication will not be able to read its content. The scheme provides message recovery and no plaintext message is transmitted to the BS. Only the BS can decrypt the message communicated after proofing its authenticity.

b) *The proposed scheme provides security against Authenticity Threats.* The messages sent from the wireless sensor nodes to the BS are signed using the private key of the sensor nodes. Any minor change in the message will alter value s, e and c. Since, the approach used for signing is $s = z \cdot (c \cdot k)$ the adversary will need to provide a value c' such that $c' = (s.z)/k$. The value z and k are private and k is a nonce that changes with every new message.

c) *Message Integrity*. If an active adversary makes changes to the massage m_i, the message will be rejected at the ciphertext authentication stage since $c = c' = H_2(e', WS_{ID_i}, BS_{pk}, vt)$ will not hold.

d) *Compromise Attack.* A compromise attack can be resisted by use of password PW . If an attacker could capture a wireless sensor node, the attacker can only get encrypted user private keys (d', z', vt'). The adversary will not be able to recover (d, z, vt) since he/she has no access to user's password PW.

e) *Secure against Replay Attack.* Assuming that the proposed protocol has a time synchronization mechanism agreed between sensor nodes WS_i and BS to enable checking for data freshness. If an adversary was to intercept message and replay it at time $tt_{i'}$, assuming that the valid time delay is given as ΔT .The WS_i and BS will receive this message and check if $tt_{i'} - tt_i \geq \Delta T$is within the allowed propagation delay time, if it is not the message is assumed to be a replay attack and dropped.

f) *Denial-Of-Service Attack*. A sensor node will only receive messages from pre-authorized sensor node based on their WS_{ID} . The broadcast message communication of any wireless sensor node that fails the verification process will promptly be discarded and reported to the BS. Each wireless sensor node is allowed to authenticate a broadcast message from one sensor node at a time. A wireless sensor node that is unable to validate the received broadcast for a given number of times in a row, it will communicate the occurrence to the BS. The BS will take the initiative of limiting its access to the WSN as it investigates the incident.

g) User Anonymity. An adversary will not be able to know the identity of the user since the sensor sends $WS_{ID} = H_4(ID)$, which is not the actual identity of the user/sensor. The message is encrypted as $e = m_i \oplus d_i \parallel F_x$ reducing the chances of knowing any information that may lead to the identity of the person associated with the sensor hence preserving user's privacy.

h) Mutual Authenticity. All communicating parties are mutually authenticated with each other. When a sensor B receives message $\{F, s, e, c, WS_{ID_i}, tt_i\}$ from sensor A it has to validate that the message transmitted was actually generated by sensor node A and vise versa. Hence mutual authentication is achieved.

i) Man-in-the-middle Attack. If an attacker intercepts a communication between nodes the attacker will not be able to masquerade as BS or WS_i. From the above discussion it is clear that the proposed protocol can provide mutual authentication and is secure against a reply attack hence, man-in-the-middle attack can be thwarted.

4.3.5 Performance Comparison

4.3.5.1 Computational Analysis

This research evaluated the computational analysis of the proposed scheme against other related schemes by (Cao et al., 2008) and (Bashirpour et al., 2018). Computational cost based on time complexity of ECC operations with regard to modular multiplication as summarized by (Bashirpour et al., 2018) in Table 10 was evaluated.

Table 10: Unit conversion of cryptographic operations

Notations	Description
T_M	Modular multiplication
T_{PA}	Elliptic curve point addition $T_{PA} = 0.12T_M$
T_{SM}	Scalar multiplication $T_{SM} = 29T_M$
T_{INV}	Modular inverse operation $T_{INV} = 11.6T_M$
T_H	One-way hash function, Negligible
T_{Add}	Modular add operation, Negligible

Table 11: Time Complexity of Schemes

Schemes	**Signature Gen**	**Time Complexity**	**Signature Verification**	**Time Complexity**
Cao et al.,2008	$T_{SM} + T_M + T_{Add} + T_H$	$30T_M + T_{Add} + T_H$	$3T_{SM} + 2T_{PA} + 2T_H$	$87.24T_M + 2T_H$
Bashirpour et al.,2018	$2T_{SM} + 2T_M + T_{Add} + T_H$	$60T_M + T_{Add} + T_H$	$2T_{SM} + T_{PA} + 2T_H$	$58.12T_M + T_H$
Proposed scheme	$T_{SM} + 2T_M + T_H$	$31T_M + T_H$	$T_{SM} + T_M + T_H + T_{Inv}$	$30.73T_M + T_H$

If T_s denotes the number of executions for signing and T_v denotes the number of signature verification in a WSN and T_x denotes the time complexity of broadcast authentication. Now given a WSN has 1000 sensor nodes then $T_v = 1000$ and $T_s = 1$. The time complexity T_x is computed as shown in Table 4 where the proposed scheme is more efficient compared to the other two schemes by (Cao et al., 2008) and (Bashirpour et al., 2018).

Table 12: Broadcast Authentication Time Complexity

Schemes	Time Complexity
Cao et al.,2008	$T_x = 30T_M + (1000 * 87.24T_M) = 87270T_M$
Bashirpour et al.,2018,	$T_x = 60T_M + (1000 * 58.12T_M) = 58180T_M$
Proposed Scheme	$T_x = 31T_M + (1000 * 30.73T_M) = 30761T_M$

As observed in Table 12, the cryptographic scheme by (Cao et al., 2008) is more computationally efficient in the signature generation than the proposed scheme and (Bashirpour et al., 2018). However, the proposed scheme is more efficient in the signature verification than the scheme by (Cao et al., 2008) and (Bashirpour et al., 2018) as shown in Table 11. The research placed more emphasis on computation cost in the verification process during the broadcast authentication process since the nodes are resource constrained. The overall complexity as shown in Table 12 computed using unit conversions in Table 10. The proposed authentication scheme is more efficient in computation than all the other two schemes listed in the Table 12.

4.3.5.2 Communication efficiency Analysis

In this research communication analysis was conducted where the proposed scheme was compared with the schemes by (Cao et al., 2008) and (Bashirpour et al., 2018) which are pairing-free cryptographic schemes based on ECC and the approach used in (Shim, 2007) is adopted. The research considered a MICAz mote (Ali et al., 2011) which has a clock speed of about 8 MHz, 8-bit processor ATmega128L and its data rate is 12.4 kbps. The operating system used is the TinyOS. The power level of the MICAz sensor is 3.0 V where the current draw in active mode is given as 8.0 mA, receiving current draw is 10 mA and the sending current draw is 27 mA (Cao et al., 2008; Wander et al., 2005).

To achieve 80 bits security level on ECC this research considers G as additive cyclic group generated by point $P = (x, y)$ on a non-singular elliptic curve $E: y^2 = x^3 + ax +$

$b \ mod \ p$ with order q . Elements in Z_q^* are of size 160 bits and the size of prime numbers a, b, p is 160 $bits$. Therefore, the elements in G is $160x2 = 320 \ bits$.The timestamp $|tt|$ and identity $|ID|$ are set each at 32 bits. Additionally, the length of message is $|M| = 160 \ bits$.

The message transmitted by the scheme by (Cao et al., 2008) is $< M, tt, ID, sig\{M, tt, ID\} >$, where $sig\{M, tt, ID\}$ is user generated signature on M, tt, ID giving an output of $\sigma =< R_i, y_i, z_i >$. The total length of transmitted message is $|M| + |tt| + |ID| + |R| + |y| + |z| = 160 + 32 + 32 + 320 + 160 + 160 = 864 \ bits$.

While the broadcast authentication scheme proposed by (Bashirpour et al., 2018) will send message $< M, tt, sig\{M, tt, ID\}, Q >$, where $sig\{M, tt, ID\}$ is generated in the signature generation phase on M, tt, ID giving an output of $\sigma =< s, F, X >$. The total length of transmitted message is $|M| + |tt| + |s| + |F| + |X| = 160 + 32 + 160 + 320 + 320 + 320 = 1312 \ bits$. The message broadcasted by the proposed scheme is $< sig\{F, s, e, c\}ID, tt >$ where the complete message transmitted is $|F| + |s| + |e| + |c| + |ID| + |tt| = 320 + 160 + 160 + 160 + 32 + 32 = 864 \ bits$. It is clear that the proposed scheme is 66% more efficient in terms of communication compared to the scheme by (Bashirpour et al., 2018) while compared to the scheme by (Cao et al., 2008) the proposed scheme has the same communication cost.

4.3.5.3 Energy Consumption Analysis

In the evaluation of the energy consumption of the proposed scheme against other related schemes by (Cao et al., 2008) and (Bashirpour et al., 2018) this research only considered point multiplication also known as scalar multiplication of the elliptic curve cryptography. The impact of communication cost on energy consumption for received and transmitted a message of n bytes are $W_r = V \times I_r \times n \times 8/r$ and $W_t = V \times I_t \times n \times 8/r$ respectively. The voltage is denoted as V while I_r denotes the current draw for receiving, I_t is the current draw for transmitting and r denotes the data rate. When a flooding method is used, a sensor wishing to broadcast its message in the WSN will only transmit once and will receive message N times, where N represents neighboring sensor nodes. Following the approach adopted by (Shim, 2007), the research assumes the message will be 80 bits. The energy consumption for sensor transmitting a message M using scheme by(Cao et al., 2008) and(Bashirpour et al., 2018) is $W_t = 3.0 \times 27 \times 864/12400 = 5.64mJ$ and $W_t = 3.0 \times 27 \times 1312/12400 = 8.57mJ$ respectively, while the proposed scheme will consume $W_t = 3.0 \times 27 \times 864/12400 = 5.64mJ$. The energy consumption for receiving a message M using scheme by (Cao et al., 2008) and (Bashirpour et al., 2018) is $W_r = 3.0 \times 10 \times 864/12400 = 2.09mJ$ and $W_r = 3.0 \times 10 \times 1312/12400 = 3.17mJ$ respectively, while the proposed scheme will consume $W_r = 3.0 \times 10 \times 864/12400 = 2.09mJ$. When a sensor node is broadcasting a message to the whole WSN, the sensor will transmit once and can receive N number of times. This will lead to a communication energy cost of $(5.64 + 2.09N)mJ$ for the scheme by (Cao et al., 2008) while the overall consumption for the scheme by (Bashirpour et al., 2018) is $(8.57 + 3.17N)mJ$ and the proposed scheme will have a total energy consumption of $(5.64 + 2.09N)mJ$ similar to that of (Cao et al., 2008). The energy consumption for running a scalar multiplication operation over a sect163k1 Koblitz curve on a MICAz mote is $7.9\ mJ$(Shim, 2007) The computation energy cost of the proposed scheme against the schemes by (Cao et al., 2008) and (Bashirpour et al., 2018) is summarized in Table 13. The scheme by (Cao et al., 2008) and the proposed scheme is more 50% efficient compared to the scheme by (Bashirpour et al., 2018). The new proposed scheme will allow a sensor node to perform ciphertext authentication without the requirement of running the whole verification process making the proposed scheme more efficient than the schemes by (Cao et al., 2008) and (Bashirpour et al., 2018). The sensor verification process of the scheme by (Bashirpour et al., 2018) is 66% more efficient in computation energy compared to the scheme by (Cao et al., 2008). The verification part of the proposed scheme is 53% more efficient in energy computation cost at the Base Station compare to the scheme proposed by (Bashirpour et al., 2018) and 33% more efficient compared to the scheme by (Cao et al., 2008).

Table 13: Computational Energy Cost

Schemes	User	Sensor	Base Station (Sink)
Cao et al.,2008	$T_{SM} + T_H$ $1 \times 7.9 = 7.9\, mJ$	$3T_{SM} + 2T_H$ $3 \times 7.9 = 23.7\, mJ$	$3T_{SM} + 2T_H$ $3 \times 7.9 = 23.7\, mJ$
Bashirpour et al.,2018	$2T_{SM} + T_H$ $2 \times 7.9 = 15.8\, mJ$	$2T_{SM} + 2T_H$ $2 \times 7.9 = 15.8\, mJ$	$2T_{SM} + 2T_H$ $2 \times 7.9 = 15.8\, mJ$
Proposed Scheme	$T_{SM} + T_H$ $1 \times 7.9 = 7.9\, mJ$	T_H -	$T_{SM} + T_H$ $1 \times 7.9 = 7.9\, mJ$

4.3.6 Summary

The proposed Broadcast Authentication scheme makes use of a light weight signature protocol based on ECDLP that can be applied on sensor networks. The scheme has message recovery and ciphertext authenticity that negates the need for sensor nodes to run the entire signature verification process. The proposed scheme was evaluated against other related broadcast authentication schemes and the proposed BA scheme was found to be more efficient in computational overhead than the other related schemes. Therefore, the proposed BA scheme is suitable for use on WSNs. The future recommended work should focus on generating an efficient signcryption scheme for resource constrained devices based on the proposed authentication scheme.

4.4 Cryptanalysis of a Pairing-free Certificateless Signcryption scheme

4.4.1 Introduction

A signcryption scheme is an important cryptographic primitive that aims to achieve confidentiality and authentication in an efficient manner. In the efforts of learning how to develop secure signcryption schemes, this research cryptanalyzed a signcryption scheme by (Wei & Ma, 2019) which is claimed to be secure and found it not secure. Further, the research proposed an improvement to the signcryption scheme that is more secure than their scheme. The security analysis provided below can be applied to other signcryption schemes with similar design.

4.4.2 Attack Model

The scheme by (Wei & Ma, 2019) follows a model described in (Seo & Bertino, 2013). The research looked at security from the perspective of two types of adversaries. The Type-I attacker who is not in possession of KGC's secret key but can replace user's public keys and is usually denoted as A_I. A Type II attacker, in an adversary that represents a malicious KGC that has access to the master secret key and is usually denoted as A_{II} under unforgeability (Huifang & Bo, 2016). In this section, the research reviews a certificateless hybrid signcryption scheme proposed by (Wei & Ma, 2019) and shows how the scheme is existentially forgeable against both Type-I and Type-II adversary.

4.4.3 Wei and Ma Signcryption Scheme

The signcryption scheme by (Wei & Ma, 2019) (hereafter called WM) is composed of six probabilistic polynomial-time algorithms: setup, set secret value, extract partial private key, set private key, signcrypt, and de-signcrypt.

4.3.3.1 SetUp

The algorithm takes parameter λ as input and returns system parameters $params$ and master key msk. The algorithm is run by the KGC. The setup is performed as follows: Choose λ -bit prime p and return tuple $\{p, F_p, G_p, P\}$, where G_p is an additive cyclic group that consists of a point on elliptic curve over F_p and P as the generator of G_p.Choose master key $x \in Z_p^*$ and set master public key as $P_{pub} = xP$, then choose cryptographic hash functions:$H_0\{0,1\}^* X G_p \rightarrow Z_p^*$, $H_1: G_p X G_p \rightarrow \{0,1\}^n$, $H_2: G_p X\{0,1\}^* X\{0,1\}^* X G_p \rightarrow Z_p^*$ and $H_3: G_p X\{0,1\}^* X\{0,1\}^* X G_p \rightarrow Z_p^*$. KGC will publish system $params = \{F_p, G_p, P, P_{pub}, H_0, H_1, H_2, H_3\}$.

4.3.3.2 Set Secret Value

The algorithm is run by $user_i$ with identity ID_i , $user_i$ randomly selects value $x_{IDi} \in Z_p^*$ and computes public key $P_{IDi} = x_{IDi}P$.

4.3.3.3 Extract Partial Private Key

KGC computes $d_{IDi} = xH_0(ID_i, P_{IDi}) mod\ p$ as the partial private key and forwards d_{IDi} to to user through a secure channel. When user receives d_{IDi}, $user_i$ can verify d_{IDi} by checking if $d_{IDi}P = xH_0(ID_i, P_{IDi})P_{pub}$ holds.

4.3.3.4 Set Private Key

The full private key is set as $sk_{ID} = (d_{IDi}, x_{IDi})$.

4.3.3.5 Signcrypt

A $user_i$ with identity ID_s and τ as timestamp, will execute the algorithm as follows:

Algorithm 7: Ciphertext Generation

```
1. Choose a random $l_{ID} \in Z_P^*$ ; $S_{ID} = l_{ID}P;\ H = H_2(S_{IDs}, \tau, ID_r, P_{IDs});$
2. $H' = H_3(S_{ID}, \tau, ID_r, P_{IDr});$
3. $W_{IDs} = d_{IDi} + l_{IDs} \cdot H + x_{IDs} \cdot H'\ mod\ p;$
4. $T_{IDS} = l_{IDs} \cdot H_0(ID_r, P_{IDr})P_{pub};$
5. $K = H_1(T_{IDS}, l_{IDs} \cdot P_{IDr})$and
   outputs $\varphi ID_s = (s_{IDs}, W_{IDs})$ and $K$
```

4.3.3.6 De-Signcrypt

Given φID_s, K , signer identity $ID_s$and public key P_{IDs}. The decryption process proceeds as follows:

Algorithm 8: Un-signcrypt

```
1. $H = H_2(S_{IDs}, \tau, ID_r, P_{IDs}),$
2. $H' = H_3(S_{IDs}, \tau, ID_r, P_{IDr})$
3. If $W_{IDs}P = H_0(ID_s, P_{IDs})P_{pub} + H \cdot S_{IDs} + H'P_{IDs}$then
   the signature is valid, the receiver recover $ID_r$ is used to
   compute $T_{IDS} = d_{IDr} \cdot\ S_{IDs}$
4. Else
   Return ⊥
```

4.4.4 Security Analysis

4.4.4.1 Unforgeability

The scheme by WM (Wei & Ma, 2019) is claimed to be existentially unforgeable against both Type-I and Type-II attacks with proof similar to Bartino (Seo & Bertino, 2013). This research shows that their scheme is insecure against both Type-I and Type-II attacks. In EUF-CMA-I and EUF-CMA-II games, A_I and A_{II} forgers have access to full private key of the receiver, A_I is not allowed to query partial private key of the sender andA_{II} is not allowed to replace public key or extract the user private key.

Type-I Attack: The adversary interacts with challenger C in the training phase similar to WM (Wei & Ma, 2019). Adversary A_I cannot make a query for the private key for the sender. However, A_I has access to receiver's full private key. Adversary A_I makes signcryption queries with ID_s, ID_r and arbitrary value τ. C responds to A_I with $\varphi_{IDs} = (S_{ID}, W_{IDs})$ and symmetric key $K^* = H_1(T_{IDS}, x_{IDr} \cdot S_{ID})$. Adversary obtains a forged $\varphi^*_{ID_s} = (S_{ID}, W_{IDs})$ during the training phase for the same arbitrary value τ by performing the following steps. A_I selects $x^*_A, d^*_A \in_R Z^*_P$ and replaces sender public key P_{ID_s} with $P^*_{ID_A} = x^*_A P$. The adversary will proceed to compute the master public key computed as$P^*_{pub} = H_0^{-1}(d^*_A P)$ such that $d^*_A P = H_0(ID_s, P^*_{ID_A})$ holds.$A_I$selects $l_{ID} \in_R Z^*_P$ and proceeds by computing $S_{ID} = l_{ID}P;\ H = H_2\left(S_{ID}, \tau, ID_s, P^*_{ID_A}\right);\ H' = H_3(S_{ID}, \tau, ID_r, P_{IDr});\ W_{IDs} = d^*_A + l_{ID} \cdot H + x^*_A \cdot H' \ mod\ p;\ T_{IDS} = d_{IDr} \cdot S_{ID}$. Finally, it will output signature $\varphi^*_{ID_s} = (S_{ID}, W_{IDs})$ and symmetric key $K^* = H_1(T_{IDS}, l_{IDs} \cdot P_{IDr})$.The signature will pass verification because $W_{IDs}P = H_0\left(ID_s, P^*_{ID_A}\right)P^*_{pub} + H \cdot S_{ID} + H' \ \cdot P^*_{ID_A}$ will hold. The scheme by WM (Wei & Ma, 2019) has a security flaw that can allow an adversary to access to KGC's master secret key x by computing $x' = d_{IDi} H_0(ID_i, P_{IDi})^{-1}$. This makes it possible to compute partial private key for a given user as $d^*_i = x' H_0(ID_i, P_{IDi}) mod\ p$. The partial private key can be verified by checking if equation $d^*_i P = H_0(ID_i, P_{IDi}) P_{pub}$ holds.

Type-II Attack: The adversary interacts with challenger C in the training phase similar to WM (Wei & Ma, 2019). A_{II} cannot query private key for sender. However, A_{II}has access to receiver's full private key. Adversary A_{II} makes signcryption queries with ID_s, ID_r and arbitrary value τ. C responds to A_{II} with $\varphi^*_{IDs} = (S_{ID}, W_{IDs})$ and symmetric key K^*. Now A_{II} has forged signature φ^*_{IDs} for arbitrary value τ obtained as follows.A_{II} computes a new key $K^* = H_1(T_{IDS}, x_{IDr} \cdot S_{ID})$ where $T_{IDS} = d_{IDr} \cdot S_{ID}$.Therefore, $\varphi^*_{IDs} = (S_{ID}, W_{IDs})$ is a valid signature of key K^* from sender ID_s and receiver ID_r. Computation of $H = H_2(S_{ID}, \tau, ID_s, P_{IDs})$will yield the same value for signature φ^*_{IDs} or φ_{IDs}. The validity check $W_{IDs}P = H_0(ID_s, P_{IDs})P_{pub} + H \cdot S_{ID} + H' \ \cdot P_{IDs}$ will hold.

4.4.5 Proposed Modification Signcryption Scheme

In this section this research is proposing a secure and efficient scheme which is a modification of the signcryption scheme by WM (Wei & Ma, 2019).

4.4.5.1 SetUp

The setup is similar to WM (Wei & Ma, 2019) except for a change in cryptographic $H_0\{0,1\}^* XG_pXG_p \rightarrow \ Z^*_p; H_1: G_pXG_pXG_p \rightarrow \{0,1\}^n$, $H_2: G_pXG_pX\{0,1\}^*X\{0,1\}^*XG_p \rightarrow Z^*_p$ and $H_3: G_pXG_pX\{0,1\}^*X\{0,1\}^*XG_p \rightarrow Z^*_p$. KGC will publish the system $params = \{F_p, G_p, P, P_{pub}, H_0, H_1, H_2, H_3\}$

4.4.5.2 Set Secret Value`

The algorithm is run by $user_i$ with identity ID_i , $user_i$ randomly selects value$x_{IDi} \in Z^*_p$ and computes public key s $P_{IDi} = x_{IDi}P$.

4.4.5.3 Extract Partial Private Key

KGC will randomly select value$r_{IDi} \in Z^*_p$ and set $R_{IDi} = r_{IDi}P$ then compute partial private key as $d_{IDi} = r_{IDi} + x \cdot h_0 \ mod \ p$ where $h_0$is $H_0(ID_i, R_{IDi}, P_{IDi})$as the partial private key. KGC computes value $Q_{IDi} = R_{IDi} + H_0(ID_i, R_{IDi}, P_{IDi})P_{pub}$ and forwards $(d_{IDi}, Q_{IDi}, R_{IDi})$ to user through a secure channel. When user receives d_{IDi}, $user_i$ can verify d_{IDi} by checking if $d_{IDi}P = R_{IDi} + H_0(ID_i, R_{IDi}, P_{IDi})P_{pub}$ holds.

4.4.5.4 Set Private Key

The full private key is set as $sk_{ID} = (d_{IDi}, x_{IDi})$.

4.4.5.5 Signcrypt

A $user_i$ with identity ID_s and τ as timestamp, will execute the algorithm as follows:

Algorithm 9: Signcrypt

```
1. Choose a random $l_{ID} \in Z_P^*$ ;
2. $S_{ID} = l_{ID}P; T_{IDS} = l_{IDs} \cdot Q_{IDr};$
3. $H = H_2(S_{ID}, T_{IDS}, \tau, ID_r, P_{IDs});$
4. $H' = H_3(S_{ID}, T_{IDS}, \tau, ID_r, P_{IDr});$
5. $W_{IDs} = d_{IDs} + l_{IDs} \cdot H + x_{IDs};$
6. $H' \ mod\ p;\ K = H_1(T_{IDS}, S_{ID}, Q_{IDr}, ID_r)$
   Output $\varphi ID_s = (S_{IDs}, W_{IDs})$ and $K$
```

4.4.5.6 De-Signcrypt

Given φID_s, K , signer identity $ID_s$and public key (Q_{IDs}, P_{IDs}). The decryption process proceeds as follows:

Algorithm 10: De-Signcrypt

```
1. $T_{IDS} = d_{IDr} \cdot\ S_{IDs}$ ;
2. $H = H_2(S_{ID}, T_{IDS}, \tau, ID_r, P_{IDs}),$
3. $H' = H_3(S_{ID}, T_{IDS}, \tau, ID_r, P_{IDr})$
4. If $W_{IDs}P = Q_{IDs} + H \cdot S_{IDs} + H' \cdot\ P_{IDs}$ then
       the signature is valid, the receiver computes
           $K = H_1(d_{IDr} \cdot\ S_{IDs}, Q_{IDr}, ID_r)$
5. **Else**
       Return ⊥
```

Correctness

The correctness of the proposed scheme is as follows:

$T_{IDr} = l_{ID}Q_{IDr} = l_{ID}(R_{IDr} + h_0P_{pub})$ while T_{IDr} can also be computed as $T_{IDr} = d_{IDr}S_{IDs} = l_{ID}P(r_r + xh_0) = l_{ID}\left(R_{IDr} + h_0P_{pub}\right)$.

4.4.6 Security analysis of the proposed scheme

The security of the new improved scheme is based on Elliptic Curve Discrete Logarithm (ECDL) problem. In this research a formal security proof that the new signcryption scheme is UF-CMA secure against Type-I and Type-II adversary in the random oracle model under ECDL assumption is given.

4.3.6.1 Proof of unforgeability

Theorem 2: *The proposed scheme is EUF-CMA secure in the random oracle model under the ECDLP assumption.*

Proof: This research provides the proof for this theorem in Lemma 1 and Lemma 2.

Lemma 1 *The proposed scheme is EUF-CMA secure under DLP assumption in random oracle model. If there exists adversary A_I with a non-negligible advantage ε that can compromise authenticity property of proposed scheme, then there exists algorithm C that can solve the DLP problem with advantage*

$Pr\,Pr\,[C]\ \geq \varepsilon\frac{1}{qH_0}\left(1-\frac{q_s(qH_2+qH_3)}{2^k}\right).$

Here, qH_0, qH_2 and qH_3 is the maximum number of queries to H_0, H_2 and H_3 queries respectively, while q_s and q_u represents signcryption and unsigncrypt queries respectively.

Initialization: After running $Setup(1^k)$, the challenger C gives the system params to adversary A_I. Value $b \in_R Z_q^*$ will be used to simulate the partial private key of the sender, therefore challenger C must solve $P = dP$ for $(Q_A = dP)$ which is an instance of ECDL problem. C maintains lists $L_i(i = 0,1,2,3)$ for random oracles H_0, H_1, H_2 and H_3. A list L_K can be used to store private and public keys.

Training Phase. In this phase hash queries are similar to *theorem 1* in (Omala et al., 2018) except for H_1 query where C checks whether tuple $(T_{IDS}, S_{ID}, Q_{IDr}, ID_r, K)$ exists in L_1. If it exists, C returns K to A_I. Otherwise, it chooses $K \in \{0,1\}^n$ return is to A_I and adds tuple $(T_{IDS}, S_{ID}, Q_{IDr}, ID_r, K)$ to list L_1.

Forgery At the end of training phase, *adversary* A_I outputs ciphertext $\sigma^* = (S_{IDs}^*, W_{IDs}^*, K^*)$with ID_S^* and ID_r^* as sender and receiver respectively. If $ID_s \neq ID^*$ then C aborts the session. Otherwise, C submits an H_2 query on $(S_{ID}^*, T = d_r S_{IDs}^*, ID_r^*, P_r^*)$ and H_3 query on $(S_{ID}^*, R_s, H^*, ID_r^*)$ to obtain another H^* and H'^* respectively. A_I will fail if any of the hash values H^* and H'^* or both are already defined in the corresponding list. The validity of ciphertext φID_s^* will determine if the adversary A_I wins the game or not.

Adversary A_I will win the game if equation 1 holds

$$wP = Q_{ID} + H^* S_{ID} + H'^* P_{IDs} \quad (1)$$

Using forking lemma (Pointcheval & Stern, 2000) it is possible to obtain another equation

$$wP = Q_{ID} + HS_{ID} + H' P_{IDs} \ (2)$$

and subtract it from equation 1 to obtain

$$\frac{w^* - wP}{H^* - H + H'^* - H'} = (b + l_i + x_s)P \qquad (3)$$

Then recover value b as follows:

$$b = \frac{w^* - w}{H^* - H + H'^* - H'} - (l_i + x_s)$$

The value b is a solution to the ECDL problem, this means C can use adversary A_I as a subroutine to obtain b from $Q_A = bP$. It is possible for C to obtain x_s from public key query and can therefore solve l_i.

Analysis The evaluation is focused in the likelihood of the following events:

E_1: Adversary A_I does not choose to be challenged on ID^*

E_2: Adversary A_I did ask private key query on ID^*

E_3: Adversary A_I did replace public key and issued a partial private key query on ID^*

E_4: Challenger C aborts in unsigncrypt query due to rejection of a valid ciphertext.

The probability that Challenger C does not abort during this game is

$Pr\,Pr\,[\neg E_1 \wedge \neg E_4] \ = \frac{1}{qH_0}\left(1 - \frac{q_s(qH_2 + qH_3)}{2^k}\right).$

Therefore,

$Pr\,Pr\,[C] \ \geq \varepsilon \frac{1}{qH_0}\left(1 - \frac{q_s(qH_2 + qH_3)}{2^k}\right).$

Lemma 2 *The proposed scheme is EUF-CMA secure under ECDL assumption in random oracle model. If there exists adversary A_{II} with a non-negligible advantage ε that can compromise authenticity property of the proposed scheme, then there exists algorithm C that can solve the ECDL problem with advantage*

$Pr\, Pr\, [C] \geq \varepsilon \frac{1}{qH_0}\left(1 - \frac{q_s(qH_2+qH_3)}{2^k}\right).$

Here, qH_0, qH_2 and qH_3 is the maximum number of queries to H_0, H_2 and H_3 queries respectively, while $q_s$and q_u represents signcryption and unsigncrypt queries respectively.

Challenger C will use adversaryA_{II} to solve(P, bP)which is an instance of ECDL problem. The adversary has access to master secret key. C provides system params to the adversary including $P_{pub} = aP$ and $P_i = \lambda P$ where value λ is unknown to C. Value a is a master secret key.

Training Phase. This phase is similar to theorem 2 declared in Lemma 1.

Forgery At the end of training phase, adversaryA_{II} outputs ciphertext $\sigma^* = (S^*_{IDs}, W^*_{IDs}, K^*)$on with ID^*_s and ID^*_r not generated by Signcrypt query. If $ID_A \neq ID^*$, challenger C aborts the session. Otherwise, C submits H_2 query on tuple $(S^*_{ID}, T = d_r S^*_{IDs}, ID^*_r, P^*_r)$ to recover value H and H_3 query on $(S^*_{ID}, R_s, H^*, ID^*_r)$ to obtain another H'.AdversaryA_{II}will fail if both$H$ and H' valuesalready exist in the respective list.

Analysis The analysis is focused in the likelihood of the following independent events:

E_1: Adversary A_{II} does not choose to be challenged on ID^*

E_2: Adversary A_{II} did ask private key query on ID^*

E_3: Adversary A_{II} aborts during the unsigncryption query as a result of a rejected valid ciphertext during the simulation.

The rest of the analysis is similar to that of the analysis section of Lemma 1.

4.4.7 Performance evaluation of the Modified Scheme

The performance of the proposed access control scheme is analyzed in comparison with schemes by WM (Wei & Ma, 2019). As in (Shim, 2013) this research adopts a running time and energy consumption on MICA2 mote equipped with ATmega128 8-bit processor clocked at 7.3728 MHz, 4KB RAM and 128KB ROM. In the quantitative analysis, operations with high computation cost such point multiplication in G_1 denoted as PM are considered. From (Shim, 2014), it is know that a PM operation takes 0.81s on an elliptic curve with 160 bits p. The signcryption algorithm of WM (Wei & Ma, 2019) performs 3PM and 6PM in the un-signcryption algorithm while the proposed scheme takes 2PM and 3PM in signcryption and un-signcryption respectively. Therefore, the computational time of the modified scheme compared to the scheme by WM (Wei & Ma, 2019) is as follows:

a) Computation time for ciphertext generation and unsigncryption in WM (Wei & Ma, 2019) are $3 * 0.81 = 2.43s$ and $6 * 0.81 = 4.86s$

b) The computation time for ciphertext generation and unsigncryption in the proposed scheme is $2 * 0.81 = 1.62s$and $3 * 0.81 = 2.43s$ respectively.

The computational time of the proposed scheme is 33% more efficient in signcryption and 50% efficient in un-signcryption in comparison to the scheme by WM (Wei & Ma, 2019).

The approach used in (Cao et al., 2008) and (Shim, 2014) is adopted to compute energy consumption. The power level of MICA2 is given as 3.0V and 12.4kbps is the data rate, 8.0mA is the assumed current draw, the transmitting mode is 27mA and the current draw for receiving mode is 10mA (Cao et al., 2008). According to (Ma, Xue, & Hong, 2014) a point multiplication operation consumes $3.0 * 8.0 * 0.81 = 19.44\ mJ$. The energy computation cost of the signcryption scheme and the un-signcryption scheme by (Wei & Ma, 2019) and proposed scheme is computed as $(3 + 6) * 19.44 = 174.96\ mJ$ and $(2 + 3) * 19.44 = 97.2\ mJ$ respectively.Therefore, the proposed scheme has reduced the energy computation cost by $(174.96 - 97.2)/174.96 = 44\%$.

4.4.8 Summary

This research has demonstrated that certificateless signcryption scheme proposed recently by (Wei & Ma, 2019) can be compromised through public key replacement and further, the research has proposed how the security scheme can be improved to avoid such kind attack and presented a modified and efficient signcryption scheme. A signcryption scheme with similar construction for computing partial private key will be vulnerable to the same attack.

4.5 Towards an Efficient Certificateless Access Control Scheme for Wireless Body Area Networks

4.5.1 Introduction

WBANs have the capability to gather environmental parameters and physiological data via sensor nodes. The sensors in WBANs are said to perform three main tasks, i.e sensing patients' vital signs, processing and communicating data (Ullah, et al., 2012). Sensors nodes monitor the environment for conditions they are set to monitor, collecting and process data before sending it to the controller or sink in its network. The sensors are designed to be invasive or they can be designed to be non-invasive. An inversive sensors is surgically inserted into a human body while the non-invasive node can be attached to the human skin (Khan & Pathan, 2018). Even though these sensors nodes are resource limited in nature, they have found a lot of use in application areas ranging from indoor deployment scenarios in homes to outdoor deployment in hostile environments where they can easily be preyed upon by attackers and compromised.

In the medical field, wireless sensors and communication technologies are increasingly being deployed in remote healthcare management (Vaniprabha & Poongodi, 2017). The potential use of sensors has been demonstrated in (Arunkumar et al.,2022) and (Chipara et al., 2009). Their studies, showed an improved detection of clinical deterioration through real-time patient monitoring. Ubiquitous healthcare monitoring improved quality of the elderly as healthcare services can be provided anytime and anywhere. Unauthorized access of medical data may cause harm that may even lead to death of patients hence, the need for effective data protection in WBANs. Wireless sensors in WBANs are resource constrained hence, designing and implementing a secure Wireless Body Area Network has particularly been a challenging task. Traditional cryptographic primitives form the core of security protocols and they consume a fair amount of energy during computation making them not suitable for use on resource constrained environments.

Elliptic Curve Cryptosystems (ECC) has gained increasing popularity in the area of public key cryptography ever since it was invented by (Kobiltz, 1987) and Victor Miller (Miller, 1985) due to its ability to generate small keys. The use of ECC grants an opportunity for development of more efficient cryptographic schemes for use on devices that use less memory and require less power consumption hence, the focus on ECC. A lot of research efforts has been devoted to addressing security issues in WBANs (Winkler &Rinner, 2014; Li, Han, & Jin, 2018). Communication in a WBAN should satisfy confidentiality, authenticity, ciphertext authenticity, integrity, anonymity and non-repudiation (Li et al., 2018; Li et al., 2010). To ensure all security goals are achieved, both signature and encryption are used in the design of security schemes. Research by (Ashraf et al., 2014) has proved signing then encrypting is not efficient and this has led to the concept of signcryption proposed by (Zheng, 1997). The process of signcryption, can satisfy message authentication, integrity and confidentiality more efficiently than encrypting then signing or vice versa (Alharbi & Lin, 2016).

Signcryption comes in the forms of public key infrastructure signcryption (PKISC), identity-based signcryption (IBSC) or certificateless signcryption (CLSC) (Saeed et al., 2017). A certificate is used in PKISC to provide a more trusted connection between the public key and the identity of the user through the certificate authority (CA) signature, this leads public key infrastructure hierarchical framework whose task is to issues and manages certificates. The use of PKI on WBANs is not effective due to use of sensors since they are resource constrained in nature. Schemes based on ID approach do not use PKI, they make use of key escrow which presents a security challenge since both sender's signing key and receiver's decrypting key are provided by PKI (Yuan, 2020). Several IBSC have been proposed (Chen & Malone-Lee, 2005; Sun et al., 2008; Li et al., 2013 and Barreto et al., 2005). In (Al-Riyami & Paterson, 2003; Barbosa & Farshim, 2008) they presented a certificateless scheme to overcome the key escrow problem found in Identity-based public key cryptography. The scheme by (Barreto et al., 2005) was used by (Li & Hong, 2016) to design access control for WBANs.

A certificateless cryptosystem makes use of a trusted third party known as the Key Generating Center (KGC) who does not have access to the full private key of the user.

However, the KGC has the capacity to compute a user's partial private key from the identity of the user and its master key. The user then generates a final full private key by combining the partial private key with some secret information (Li et al., 2013). Since CLSC was introduced in 2008, a vast majority of access control schemes for WBANs have been proposed based on bilinear pairing (Cagalaban & Kim, 2011; Li & Hong, 2016). Numerous researchers have discussed how to speed up the pairing computation (Barreto et al., 2004) and (Freeman et al., 2010). However, the cost of computing a bilinear pairing operation in cryptography is still resource-consuming, especially when used in resource constrained environments. This research work is focused on pairing-free cryptography when designing the proposed access control scheme for WBANs.

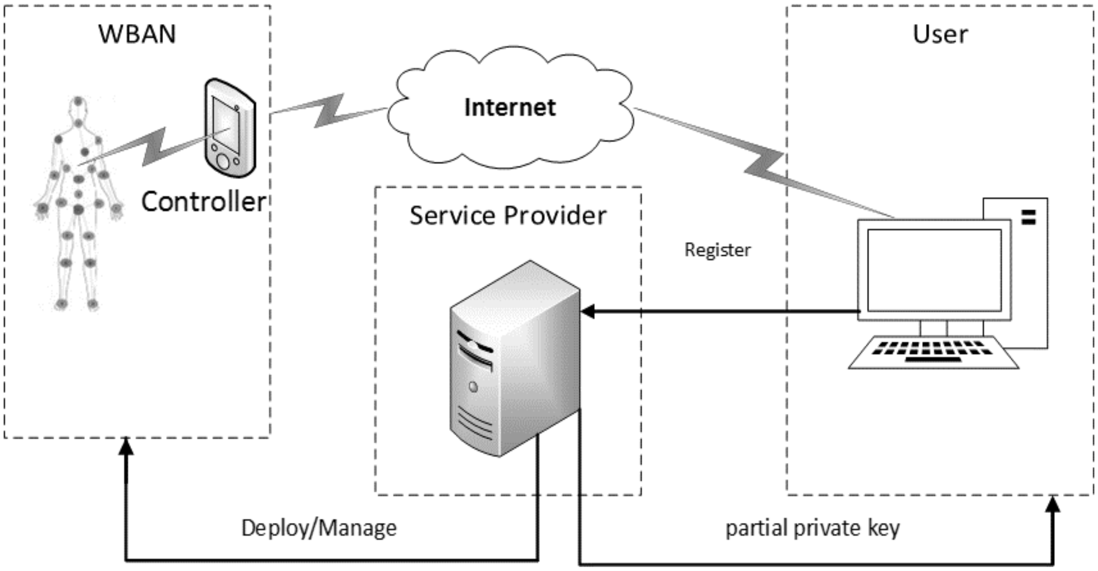


Figure 9: Network Model

Table 14: List of Notations

Symbol	Description
KGC	Key generator center
k	Security parameter
s	Master secret key of KGC
G	Cyclic group
P	Group generator
F_q	Prime field
$E(F_q)$	Elliptic curve over prime field
$H_i()$	Hash function where $i = 1,2,3$
ID_s	Identity of sender
ID_r	Identity of receiver
d_i, x_i	Full private key, i.e partial private key and secret key respectively, where $i = r, s$
pkv	Public key verification token
P_{pub}	Master public key of KGC
P_s	Public key of sender
P_r	Public key of receiver
SP	Service Provider
m	Plaintext message
σ	Ciphertext

4.5.2 Proposed CLSC scheme for WSNs

In this section, this research presents a new novel lightweight certificateless signcryption scheme that is composed of the following actors:

(1) Sender: The sender ID_s is the device that generates and communicates the message.

(2) Receiver: The receiver ID_r is the device that receives and decrypts the message communicated.

(3) Key Generation Center (KGC), who provides element of validity and trust for both parties.

The proposed certificateless signcryption scheme is made up of the following algorithms: ***Set-Up:***KGC is required to select an elliptic curve $E(F_q)$ over finite field F_q where $E(F_q)$ is defined by system parameters. KGC defines a secure cryptographic hash functions level $H_1: \{0,1\}^* \times G \times G \rightarrow Z_q^*$, $H_2: \{0,1\}^n \times G \times \{0,1\} \times \{0,1\} \rightarrow Z_q^*$where n is an integer value define from input security and $H_3: G \times G \times \{0,1\}^* \rightarrow Z_q^* KGC$ Chooses randomly a secret master secret key $s \in_R Z_q^*$ and computes general public key$P_{pub} = s.P$. KGC keeps s as a secret and publishes the system parameters as $params = \{G, P, q, P_{pub}, H_1, H_2, H_3\}$. The sender and receiver are uniquely identified by device identity ID_s and ID_r respectively.

***Set-public-key*:** On input of user's secret keyx_i , a user will compute public key as $P_i \leftarrow x_i \cdot P$ then avail the P_i to the KGC.

Set-partial-private key: This algorithm takes the secret key s , user's public key P_i and $params$ to output partial private key $d_i$for a user. The algorithm is run by the KGC where the partial private key for $user_i$ is computed as $d_i = s.H_1\left(ID_i, P_i, P_{pub_i}\right) mod\ q$ and secretly sends d_i to $user_i$ over a secure channel. A user's partial private key d_i can be verified by checking whether $d_i \cdot P = H_1(ID_i, P_i, P_{pub})P_{pub}$ holds. For the purpose of validating a user public key the KGC will compute $pkv_i = s \cdot H_1(ID_i, P_i, P_{pub})\ mod\ q$ as public key verification token pkv_i for both sender and receiver, who will use it to verify each other's public key by checking if equation $pkv_i \cdot P = P_{pub_i} \cdot H_1\left(ID_i, P_i, P_{pub_i}\right)$ holds.

Set-Secret-key: The algorithm is run by $user_i$, who will use his secret value x_i to computes $z_i = d_i^{-1} \cdot x_i^{-1}\ mod\ q$ as the second secret key then set the full private key as $SK_s = (d_i, x_i, z_i)$.

CLSC Signcryption: With system $params$, receiver's public key P_r and identity ID_r, sender's public key P_s and identity ID_s. The signcryption process proceeds as follows:

Algorithm 11 CLSC Signcryption

```
$Input: \{\ params, P_r, P_s, ID_r, ID_s\}$
Output:{ $\gamma, c, h$}
Select random parameter $r \in_R Z_q^*; W \leftarrow rP$ ;
Compute $\beta = r \cdot P_r$;
Compute $h_3 = H_3(W, \beta)$;
$Compute\ c \leftarrow h_3 \oplus m$;
$Compute\ h = H_2(W, c, P_s, P_r, ID_s, ID_r)$;
Compute $\gamma = (h \cdot d_s \cdot r) \cdot z_s\ mod\ q$.
Output signcryption text $\sigma = (\gamma, c, h)$
```

***CLSC Unsigncryption**:* After receiving signcryption text σ and taking sender's public key P_s , sender's identity ID_s and receiver's private key x_r the unsigncryption process will proceed as follows:

Algorithm 12 CLSC Unsigncryption

```
$Input: \{\ params, \gamma, c, h\}$
Output:{ $m'$}
$Compute\ Q = (\gamma \cdot h^{-1}\ mod\ q) \cdot P_s$;
$h' = H_2(Q, c, P_s, P_r, ID_s, ID_r)$;
if $h = h'$ holds then
    Compute $\beta \leftarrow x_r \cdot Q$
    return $m' = H_3(Q, \beta) \oplus c$.
else
    output symbol $\perp$
end if
```

The proposed scheme has a property of ciphertext authenticity and public verifiability. A third party is able to verify the validity of ciphertext $\sigma = (\gamma, c, h)$ produced by the proposed signcryption scheme without the knowledge of receiver's private key and the knowledge of the message m by executing the first three steps of the proposed CLSC scheme.

Correctness of the Scheme

The correctness of the proposed scheme is as follows:

$$\begin{aligned} Q &= (\gamma \cdot h^{-1}\, mod\, q) \cdot P_s \\ &= (h \cdot d_s \cdot r) \cdot z_s\ \cdot h^{-1}\ \cdot P_s \\ &= (r \cdot x_s^{-1}) \cdot P_s \\ &= r \cdot P = W \end{aligned}$$

$$\begin{aligned} \beta &= r \cdot P_r \\ &= r \cdot x_r \cdot P \\ &= x_r \cdot r \cdot P \\ &= x_r \cdot Q \end{aligned}$$

4.5.3 Security analysis of the proposed scheme

In this subsection, this research provides a formal security proof that the proposed signcryption scheme is IND-CCA2 and UF-CMA secure against Type-I and Type-II attacker in the random oracle model under Discrete Logarithm assumption.

Type-I adversary: This adversary represents an outsider adversary that does not have access to the secret master key and is usually denoted as A_I.*Type II adversary***:** Is an adversary represents an insider adversary who has access to the master secret key, denoted as A_{II}. The random oracle model is a formal model used for the purpose of analyzing cryptographic schemes, where a hash function is considered as a black box that contains a random function (Bellare & Rogaway,1996).

Theorem 1: *In random oracle model if adversary A_1 against IND-CLSC-CCA2 security of the proposed CLSC scheme will succeed with advantage ε, there will be an algorithm*

C that solves the DL problem with advantage $Adv_{A_{i(i=1,2)}}^{IND-CLSC-CCA2} \geq \frac{\varepsilon}{q_3}\left(1-\frac{1}{q_s+1}\right)^{q_s}$. Here, the adversary $A_{i(i=1,2)}$ performs at most q_i to random oracles $H_{i(i=1,2,3)}$ and q_s signcryption queries.

Proof: Assume that algorithm C who is a challenger attempts to solve DL problem by taking random instance (P, bP) as input. In order to determine b from interactions with adversary $A_I. C$ does not know the values of $b \in Z_p^*$. The game between C and adversary A_I is as follows:

***Setup*:** The challenger C runs Setup algorithm using security parameter k to generate system $params = (G, P, q, Ppub, H_1, H_2, H_3)$ and forwards the $params$ to A_I. The challenger C maintains lists L_{PK} ,L_D , L_{SK} ,L_S and L_{US} to store and track public key, partial private key, secret key, signcryption and unsigncryption queries respectively. C also maintains L_1, L_2 and $L_3$to track H_1, H_2 and H_3 oracles respectively. A list L_{rec} is used to record parameters for the challenge stage.

***Find Stage**:* Adversary A_I adaptively makes polynomial bounded number of queries as follows:

H_1 ***Queries:*** When A_1 submit a query with identity ID_i, the challenger C will check if tuple $(ID_i, P_i, P_{pub}, h_1, v)$ exists in list L_1.If it exists, then C returns h_1 to A_1. Otherwise, C selects a random $v \in_R \{0,1\}$ where $Pr\, Pr\, [v = 1] = \delta = 1/(q_s + 1)$. When $v = 0$, C randomly chooses $h_1 \in_R Z_q^*$ and returns it to A_1 then inserts tuple $(ID_i, P_i, P_{pub}, h_1, v)$ into list L_1. When $v = 1$, C sets $h_1 = k$ and returns k to adversary A_1.

H_2 ***Queries:*** When challenger C receives query with identity ID_i from adversary A_1, challenger C checks if tuple $(W, c, P_s, P_r, ID_s, ID_r, h_2)$ is in list L_2. If such a tuple exists, C returns h_2 to adversary A_1. Otherwise, challenger C randomly selects $h_2 \in_R Z_q^*$, returns h_2 to A_1 as a response to the query then inserts tuple $(W, c, P_s, P_r, ID_s, ID_r, h_2)$ in list L_2.

H_3 **Queries:** When challenger C receives query $H_3(W, \beta)$ from A_1, C checks if tuple (W, β, h_3) exist in list L_3. If it exists, C returns h_3 to adversary A_1. Otherwise, C randomly selects $h_3 \in_R Z_q^*$, returns h_3 to A_1 as a response to the query and inserts tuple (W, β, h_3) in list L_3.

Private Key query: Adversary submits a request with identity ID_i. The challenger C checks if tuple (ID_i, SK) exists in list L_{SK}. If it exists, the challenger C returns SK to A_1 where $SK = (x_i, z_i)$. Otherwise, C obtains z_i through d_i from partial private key queries, randomly picks $x_i \in_R Z_q^*$ then adds tuple (ID_i, SK) in list L_{SK} and returns SK to A_1.

Public key query: If A_1 issues public key query for identity ID_i, C first scans list L_{PK} to check whether a matching P_i for identity ID_i exists. If it exists, C returns P_i to adversary A_1. Otherwise, C checks list L_{SK}. If there exists a record for ID_i in L_{SK}, C obtains x_i then computes $P_i = x_iP$ and returns P_i to A_1 and inserts (ID_i, P_i) in list L_{PK}. If there exists no record of ID_i in list L_{SK}, C checks list L_1. If $v = 1, C$ randomly picks $x_i \in_R Z_q^*$, computes $P_i = x_iP$ and returns P_i to A_1. C then will insert tuple (ID_i, x_i, v) into list L_{rec}. If $v = 0$, C runs private key query and obtains P_i, returns P_i to $A_1$and inserts tuple (ID_i, P_i) into list L_{PK}.

Partial Private Key query: Adversary A_1 issues a partial private key query for identity ID_i, C will check list L_D for partial private key corresponding to identity ID_i. If it exists, it returns d_i to A_1. Otherwise, C selects random $d_i \in_R Z_q^*$ then returns it to A_1 . The validity of d_i can be easily be verified by checked if equation $d_iP = H_1(ID_i, P_i, P_{pub})P_{pub}$ holds. C adds tuple (ID_i, d_i) in list L_D.

***Replace Key query*:** Adversary A_1 may perform public key replacement query by submitting values (ID_i, P_i') of its choice. C checks list L_{PK} for corresponding P_i of the identity ID_i. If it is found it is replaced with a new public key P_i'.

Signcrypt Query(Q_s): The assumption is that adversary A_I made public key queries and H_1 queries before signcryption query. The challenger C checks list L_1 for (ID_s, P_s) and responds as follows:

If $v = 0, C$ fails and aborts simulation else if $v = 0, C$ gets (ID_s, d_s, z_s) , (ID_r, P_r) from list L_{SK} and L_{PK} respectively using ID_r and ID_s. Adversary C runs sign algorithm to complete signcryption ad returns ciphertext $\sigma = (\gamma, c, h)$ to A_I.

Unsigncrypt Query (Q_u): Adversary A_I may perform an unsigncrytion query on σ sender identity ID_s and receiver identity ID_r. C checks for (ID_r, P_r) in list L_1 and responds as follows:

a) If $v = 0$, C gets (ID_s, P_s) from list L_{PK} and (ID_s, SK_s) from list L_{SK} then runs unsigncryption algorithm to complete unsigncryption and returns message m to A_I.

b) If $v = 1$, C gets (ID_s, P_s) from list L_{PK} then selects h_2 from tuple $(Q, P_s, c, ID_s, ID_r, h_2)$ from list L_2. The adversary A_I will traverse (Q, W, h_3) from a matching W for the $Q \leftarrow h_2$ and computes $m' = h_3 \oplus c$ then checks if $c = h_3 \oplus m'$ holds. If it holds, C will output the message m else C will start from the next record in L_3 and repeats process (b) until all entries have been checked and returns $\perp$ if unsigncryption is unsuccessful.

Challenge: Adversary A_I will choose and output two messages (m_1, m_2) of equal length together with sender's ID_s and receiver's ID_r on which it wishes to be challenged. C will check (ID_r, P_r) from list L_1. If $v = 0$, C stops. Otherwise, C makes public key queries to ensure x_r already exists in L_{rec} list. C will then randomly values $y^*, c^*, h^* \in_R Z_q^*$ and sends a challenge ciphertext $\sigma^* = (\gamma^*, c^*, h^*)$ to adversary A_I.

Guess stage: Adversary A_I can make polynomial bounded queries just like in the Find stage. Adversary A_I returns its guess. The challenger C will ignore the guess and select a random entry of tuple (Q^*, W^*, h_3^*) in list L_3 and returns Q^* as a solution to the DL instance where $Q^* = r^* \cdot P = aP$. The ciphertext σ^* given to adversary A_I is distributed randomly in ciphertext space, the adversary has no advantage in the simulation. Algorithm C simulates an attack scenario for A_I. If C is not terminated in the process of simulation and can breach confidentiality with non-negligible probability ε, C outputs a valid answer of DL problem.

The probability of C does not abort during simulation is at least $\frac{\varepsilon}{q_3}\left(1 - \frac{1}{q_s+1}\right)^{q_s}$.

If algorithm C does not abort in the simulation process and A_I can break confidentiality of the proposed signcryption scheme with non-negligible advantage ε , C can output valid solution of DL problem with advantage $Adv_{A_1}^{IND-CLSC-CCA2} \geq \frac{\varepsilon}{q_3}\left(1 - \frac{1}{q_s+1}\right)^{q_s}$.

Theorem 2: *In random oracle model if adversary A_2 against IND-CLSC-CCA2 security of the proposed CLSC scheme will succeed with advantage ε, there will be an algorithm*

C that solves the ECDL problem with advantage $Adv_{A_{i(i=1,2)}}^{IND-CLSC-CCA2} \geq \frac{\varepsilon}{q_3}\left(1-\frac{1}{q_s+1}\right)^{q_s}$. *Here, the adversary* $A_{i(i=1,2)}$ *performs at most* q_i *to random oracles* $H_{i(i=1,2,3)}$ *and* q_s *signcryption queries.*

Proof: Challenger C takes as input (P, bP) and attempts to compute b in order to solve DL problem utilizing A_2 in the game. The proof is very similar to the proof in theorem 1 except adversary A_2 cannot issue Replace public key query. Adversary A_2 knows the master secret key s. The challenger C will ignore guess from the adversary and select a random entry of (Q, W, h_3) from list L_3 and returns W as a solution to DL problem $W^* = r^* \cdot P = bP$

4.5.3.1 Proof of Unforgeability

Theorem 3: *In random oracle model, if there exists an adversary*$A_{i(i=1,2)}$ *who can win the EUF-CLSC-CMA game of the proposed scheme with non-negligible advantage* ε, *there will be an algorithm C that solves the ECDL problem with advantage* $Adv_{A_{i(i=1,2)}}^{IND-CLSC-CMA} \geq \frac{\varepsilon}{q_1}\left(1-\frac{1}{q_s+1}\right)^{q_s}$. *Here, the adversary* $A_{i(i=1,2)}$ *performs at most* q_i *to random oracles* $H_{i(i=1,2,3)}$ *and* q_s *signcryption queries.*

Proof: If there exists adversary $A_{i(i=1,2)}$ who can break the proposed CLSC. An algorithm C is build that uses $A_{i(i=1,2)}$ to solve DL problem where algorithm C receives (P, aP) of ECDL problem with the goal to compute value a. C sets $P_{pub} = aP$ for A_1. The other settings remain as set in theorem 1 for adversary A_1 and $P_{pub} = sP$ for adversary A_2 while other settings remain as set in theorem 2 for A_2. A_1 makes polynomial bounded queries adaptively like in theorem 1 while A_2 makes queries adaptively like in theorem 2. After a polynomial bounded number of queries, $A_{i(i=1,2)}$ outputs fake ciphertext $\sigma^* = (\gamma^*, c^*, h^*)$ for message m^* with ID_s as sender and ID_r as receiver.

The challenger C first checks list L1. If $v = 0$, C aborts. Otherwise, C gets private key of ID_r and computes $\beta^* = x_r\left(y^* \cdot {h^*}^{-1} \bmod q\right)P_s$ and gets W^* for a matching β^* from h_3. Challenger C receives m^* by h_3 and verifies σ^*. If $A_{i(i=1,2)}$ successfully forged a user, C can get two signatures $(W^*, h, c^*, ID_s, ID_r, y_1)$ and $(W^*, h', c^*, ID_s, ID_r, y_2)$ with splitting lemma (Shao & Gao, 2014) when $h \neq h'$. $W^* = y.H_1 rP = y_2 H_1 rP$ in $A_1, W^* = akrP$ where $k = H_1(ID_s, P_s, P_{pub})$ only r is unknown and can be computed. The probability that A_1 runs partial private key queries for ID_s is at least $1/q_1$. The probability that it does not terminate is $(1-\delta)^{q_s}$ in the find stage. Therefore, the probability that C can solve the ECDL problem is at least $1/q_1$. The probability that C successfully forges a user is at least $\frac{\varepsilon}{q_1}\left(1-\frac{1}{q_s+1}\right)^{q_s}$.

Table 16 shows security properties of the proposed scheme again other related schemes by GPJ (Gao et al., 2019), LHJ (Li et al., 2018) and LH (Li & Hong, 2016).

4.5.4 Access Control Scheme

In this section the research shows how the proposed signcription scheme can be applied in an access control scheme for WBANs. The proposed certificateless access control scheme is composed of the following four phases: (1) Initialization phase (2) Registration phase (3) Authentication phase and (4) revocation phase as depicted in Figure 10.

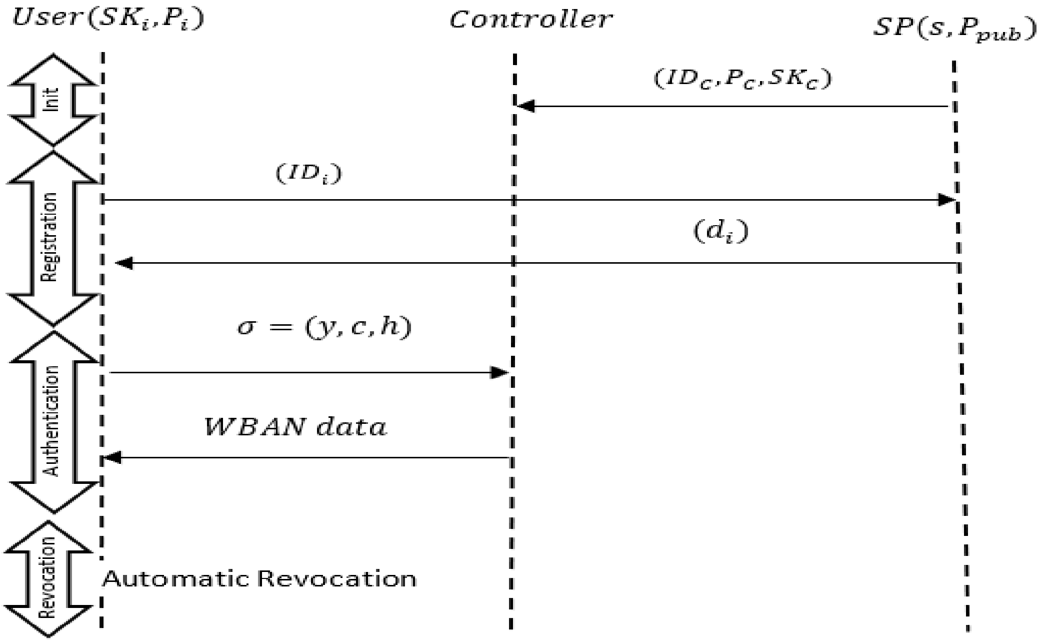


Figure 10: Certificateless Access Control Scheme

4.5.4.1 Initialization Phase

The SP acting as a KGC is in charge of running the setup algorithm to generate system $params$,its master secret key and its public key. The controller will be assigned a unique identity ID_C , public key P_C and a full private key $SK_C = (d_C, z_d)$. The private key will be delivered to the controller through a secure channel.

4.5.4.2 Registration

All the users will be required to register with the SP before they can access the WBAN. A user will select a secret value x_i and execute the public key algorithm to generate his/her public keyP_i .The user will submit his/her identity $ID_i$and public key$P_i$to the SP. The SP checks the validity of the identity ID_i , if it is not valid the registration request is rejected else SP will run the partial private key algorithm to generate partial private key d_i for the user. An expiration date ED is set and d_i is forwarded to the user. When the user receives d_i he/she can check validity of the key by checking if equation $d_i \cdot P = P_{pub_i} \cdot H_1\left(ID_i, P_i, P_{pub_i}\right)$ holds.

4.5.4.3 Authentication and Authorization Phase

When a user with identity ID_i wants to access monitoring data of a WBAN. The user will signcrypt a request service message m to generate ciphertext $\sigma = (\gamma, c, h)$. A timestamp t_i is used to resist the replay attack, where t_i will denote the current timestamp. The user will send the ciphertext, its identity, its public key and current timestamp t_i as $< \sigma, ID_i, P_i, t_i >$ to the controller. When the controller receives the transmission, it will verify the validity of the public key by computing $pkv_s \cdot P = P_{pub_i} \cdot H_1(ID_i, P_i , P_{pub_i})$. If the equation does not hold, the request is immediately rejected. Otherwise, the controller computes $Q = (\gamma \cdot h^{-1} \, mod \, p) \cdot P_i$. The proposed scheme has the advantage of both public verifiability of ciphertext and ciphertext authentication where the controller can check the validity of the ciphertext before proceeding with the decryption process by checking if $h' = H_2(Q, c, P_s, ID_s, ID_r) = h$ holds. If the equation does not hold, the ciphertext is rejected and there will be no need to proceed to step 4 of decryption, this saves on energy consumption and computation cost. Otherwise, if the equation holds the controller proceeds to compute $\beta \leftarrow x_c \cdot Q$ and recovers message $m = H_3(Q, \beta) \oplus c$. At this point, the user is allowed access to the WBAN data. The controller will from this point encrypt the WBAN data using some symmetric cipher with the session key set to be $H_3(Q, \beta)$. The session key is only known by the user requesting WBAN data and the controller. The proposed scheme is able to achieve confidentiality, non-repudiation, authenticity and integrity. If user anonymity is required it can be achieved by concatenating the identity and public key of user as $c \leftarrow h \oplus (ID_i||P_i||m)$.

4.5.4.4 Revocation Phase

The controller keeps a list of all revoked users where the revocation phase makes use of expiration data denoted as ED. Every entity in the network is assigned an ED set as the current timestamp or date during the registration process. When the ED expires, user cannot gain access to WBAN data. If there is urgent need to revoke a user's access privilege before the expiry of ED due to some reasons, the SP can send the revoked user identity to the controller.

Table 15: Computational Cost

Schemes	User	Controller
GPJ	3M	4M
LHJ	1E+4M	2P+2M+1E
LH	2E	1P+1M+1E
Ours	2M	2M

4.5.5 Performance evaluation of the Access Control Scheme

In this subsection, the research evaluates the efficiency of the proposed scheme in comparison with GPJ (Gao et al., 2019), LHJ (Li et al., 2018) and LH (Li & Hong, 2016) schemes in terms of energy consumption, communication overhead and computational cost on a MICA2 mote. In computational cost this research intents to consider only point multiplication in G_1, pairing operation and exponentiation in G_2 . Arithmetic operations and hash function will not be considered since they do not have high computational cost

(Cui et al., 2007). A MICA2 mote is equipped with ATmega128 8-bit processor functioning at 7.3728 MHz, 4KB RAM and 128 KB ROM. A point multiplication operation takes 0.81s on an elliptic curve with 160 bits p (Gura et al., 2004). An exponential operation takes 0.9s and a pairing operation takes 1.9s given η_T pairing defined on a subgroup of the 254-bit prime order of a super singular curve $y^2 + y = x^3 + x$ over $F_{2^{271}}$ with an embedded degree of 4. In (Ma et al., 2014) a point multiplication over supersingular curve will consume 0.81 s and exponentiation operation in G_2 will consume 0.9. In the analysis only the cost of the controller is considered since it is more resource limited. Therefore, the computational time of the control sensor in GPJ (Gao et al., 2019), LHJ (Li et al., 2018) ,LH (Li & Hong, 2016) and the proposed scheme are: $4 \times 0.81 = 3.24s$, $2\times 1.9 + 2 \times 0.81 + 1 \times 0.9 = 6.32\, s$, $1\times 1.9 + 1 \times 0.81 + 1 \times 0.9 = 3.61\, s$ and$2 \times 0.81 = 1.62s$ respectively. Figure 11. Shows that the proposed scheme has the least computational time compared to the schemes by GPJ (Gao et al., 2019), LHJ (Li et al., 2018) and LH (Li & Hong, 2016).

MICA2 power consumption is calculated as $W = V * I * T$ where W denotes power in millijoules, voltage is represented by V, the current draw is denoted by I in milliamps $(mA)$and T denotes time in milliseconds(ms). According to (Lynch & Kenneth, 2006; Shim et al., 2013), MICA2 current draw is $8.0\, mA$ and has a battery voltage of 3.0V. Given a point multiplication operation takes 0.81s on an elliptic curve with 160 bits p (Gura et al., 2004), the energy consumption of a point multiplication operation is computed as $3.0 * 8.0 * 0.81 = 19.44\, mJ$ and the consumption of a pairing operation will be computed as $3.0 * 8.0 * 1.9 = 45.6\, mJ$ and the consumption of an exponentiation operation in G_2 is $3.0 * 8.0 * 0.9 = 21.6\, mJ$.

Therefore the energy computation on the controller for GPJ (Gao et al., 2019), LHJ (Li et al., 2018) ,LH (Li & Hong, 2016) and the proposed access control scheme will be $4 \times 19.44 = 77.76\, mJ$, $2\times 45.6 + 2 \times 19.44 + 1 \times 21.6 = 151\, mJ$, $1\times 45.6 + 1 \times 19.44 + 1 \times 21.6 = 86\, mJ$ and $2\times 19.44 = 38.88\, mJ$ respectively. The proposed scheme has reduced energy computation as follows: In GPJ (Gao et al., 2019)$(77.76 - 38.88)/77.76 = 50\%$, in LHJ (Li et al., 2018)$(151 - 38.88)/151 = 74\%$, and LH (Li

& Hong, 2016)$(86 - 38.88)/86 = 55\%$. Figure 5 depicts energy consumption of the schemes.

In computing the communication cost, it is assumed that $|m|$20 bytes, $|ID|$= 10 bytes, |*hash*|=20 bytes and the size of a certificate is given as 86 bytes. The scheme by LHJ (Li et al., 2018) and LH (Li & Hong, 2016) use a curve over binary field $F_{2^{271}}$ with G_1 of 252 bits prime order. As in (Shim et al., 2013) the size of elements in G_1 is 542 bits and G_2 of 1084 bits, the elements in G_1 can be compressed to 34 bytes. Therefore, the cost of communication received by the controller in GPJ (Gao et al., 2019), LHJ (Li et al., 2018) and LH (Li & Hong, 2016) and the proposed scheme is as follows:

- In GPJ (Gao, Peng, & Jin, 2019) the scheme will transmit, $5|Z_q^*| + |ID| + |m|$=5*32+10+20=190 bytes.
- In LHJ (Li, Han, & Jin, 2018) the scheme will transmit, $3|G_1| + |ID| + |m|$=3*34+10+20=132 bytes
- In LH (Li & Hong, 2016) the scheme will transmit, $|G_1| + |G_2| + 3|Z_q^*| + |ID| + |m|$=34 + 136 + 3 * 32 + 10 + 20 = 296 bytes.
- In the proposed scheme will transmit, $3|Z_q^*| + |ID| + |m|$=2*32+10+20=126 bytes.

Therefore, the proposed scheme has reduced communication overhead as follows: In GPJ (Gao et al., 2019)$\frac{190-126}{190} = 34\%$, in LHJ (Li et al., 2018)$\frac{132-126}{132} = 4.5\%$ and LH (Li & Hong, 2016)$\frac{296-126}{296} = 57.4\%$. Figure 12 depicts energy consumption of the schemes.

Table 16: Comparisons of security properties

Schemes	Confidentiality	Integrity	Authenticity	Non-Repudiation	Cipher Authenticity	No Certificate	No Escrow	Without Pairing
GPJ	Y	Y	Y	Y	N	Y	Y	N
LHJ	Y	Y	Y	N	Y	Y	Y	Y
LH	Y	Y	Y	Y	Y	Y	Y	N
Ours	Y	Y	Y	Y	Y	Y	Y	Y

Abbreviations: Y: Scheme satisfies the attribute, X: Scheme fails to satisfy the attribute.

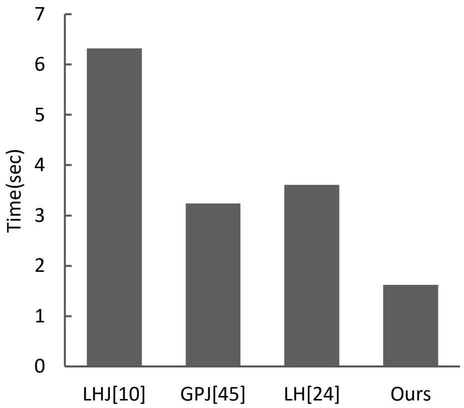


Figure 11: Computational Time of the controller

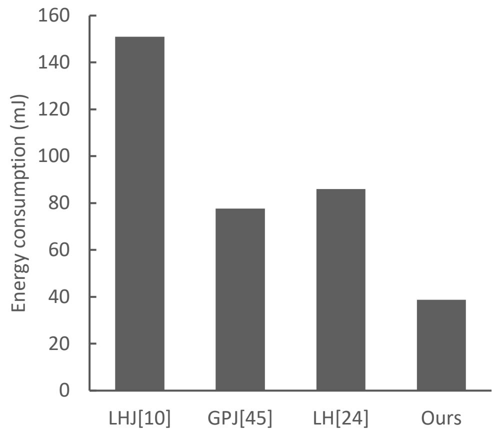


Figure 12: Energy consumption of the controller

4.5.6 Summary

This research has proposed a pairing free certificateless signcryption scheme and used it in the design of an efficient access control scheme. The proposed signcryption scheme is based on the proposed digital signature in subsection 4.2.2. The access control scheme is able to satisfy ciphertext authenticity among other security properties as discussed in this research. Further, the proposed access control scheme is computationally efficient and therefore suitable for use on resource constrained environments such as WBANs.

4.6 Certificateless Signcryption Scheme for Wireless Sensor Networks

Wireless Sensor networks have found use in Ubiquitous Healthcare Monitoring (UHM) systems as demonstrated in (Arunkumar et al., 2022). UHM has the potential to support disease management enabling patients to live an independent life where monitoring and treatment of patients can be done from a remote location (Mukherjee & Mukherjee, 2019). UHM makes use of Wireless Body Area Network (WBAN) which is simply a body sensor network designed to autonomously connect sensors and appliances. The privacy of digital data is one of the most important issues of digital advancement. There is a need to ensure data collected, processed or transmitted in a UHM system is protected from unauthorized access, especially when it comes to Patient Generated Health Data (PGHD).

This thesis proposed another certificateless signcryption scheme whose construction is based on the proposed ECDSA variant discussed in section 4.2.2. This research proposed as certificateless pairing free signcryption scheme is defined by the following seven algorithms:

1. **Set-Up:** Given the security parameter μ , the KGC will be required to select an elliptic curve $E(Fq)$ over finite field F_q where the $E(F_q)$ is defined by the chosen system parameters. KGC defines a secure cryptographic hash functions level:

   $H_0: \{0,1\}^* XG^2 \rightarrow Z^*{}_P$, $H_1: \{0,1\}^\mu XG^3 X\{0,1\}^* X\{0,1\}^* \rightarrow Z^*{}_P$ and $H_2: G^3 XZ^*{}_P \rightarrow \{0,1\}^*$. Here $\mu = |m|$ is the length of the message to be sent. KGC Chooses randomly a master secret $msk \in_R Z_p^*$ and computes general public key $P_{pub} = msk \cdot P$. KGC publishes the system parameters as $params = \{p, P, G, P_{pub}, H_0, H_1\}$ and keeps the master secret key msk as a secret. The sender and receiver are uniquely identified by device identity ID_s and ID_r respectively.

2. **Partial-private key Extract:** This algorithm takes the secret key msk and params to output partial private key d_i for a user. The algorithm is run by the KGC where the partial private key for $user_i$ is computed as $d_i = r_i + msk \cdot H_0(ID_i, R_i, P_{pub}) \bmod q$ and secretly sends d_i and R_i to $user_i$.The partial private key $d_i$can be verified by checking whether $d_i P = R_i + H_0(ID_i, R_i, P_{pub}) P_{pub}$ holds.
3. **Set-Secret-key:** The algorithm is run by $user_i$ who will randomly select a secret value $x_i \in Z^*{}_P$.
4. **Set-public-key:** The public key generation is executed by a $user_i$. The $user_i$ computes $PK_i \leftarrow d_i \cdot x_i \cdot P$ where the sender's full public key is set as $P_r = (PK_r, R_r)$.
5. **Set-full-private key:** $user_i$ will set the full private key as $FPK_i = (d_i, x_i)$.
6. **CLSC Signcryption:**
   (a) Select random parameter $k \in_r Z_P{}^*$; $W \leftarrow kP$;

(b) Compute $\beta = k \cdot PK_r$;

(c) Compute $c_0 = H_1(m, PK_s, \beta, R_r, ID_s, ID_r)$

(d) Compute $v = c_0 \cdot k \cdot (d_s \cdot x_s)^{-1} mod\ q$

(e) Compute $c_2 = H_2(W, \beta, R_s, v)$

(f) Compute $c_1 \leftarrow E_{C2}(m)$.

(g) The sender will output signcryption text $\psi = (v, c_1, c_0)$

7. **CLSC Unsigncryption**:

After receiving signcryption text ψ the unsigncryption process will proceed as follows:

(a) Compute $Q = (v \cdot {c_0}^{-1}\ mod\ q) \cdot PK_r$

(b) Compute $\beta \leftarrow (d_r \cdot x_r) \cdot Q$

(c) Compute $c_2 = H_2(Q, \beta, R_s, v)$

(d) Compute $m = D_{C2}(c_1)$

(e) ${c_0}' = H_1(m', PK_s, \beta, R_r, ID_s, ID_r)$

(f) Accept message m iff ${c_0}' = c_0$ else return $\perp$

Correctness:

The correctness of the scheme is as follows:

$$Q = (c_0 \cdot k \cdot (d_s \cdot x_s)^{-1}) \cdot (c_0)^{-1} \cdot PK_s = (k \cdot (d_s \cdot x_s)^{-1})$$

$$PK_s = (k \cdot d_s \cdot x_s \cdot (d_s \cdot x_s)^{-1}) \cdot P = k \cdot P = W.$$

and

$$\beta = d_r \cdot x_r \cdot Q = d_r \cdot x_r \cdot kP = kPK_r$$

4.6.1 Security Analysis

The signcryption scheme is IND-CCA2 and EUF-CMA secure against Type-I and Type-II attacker in the random oracle model under Computational Diffie-Hellman (CDH) assumption and Discrete Logarithm assumption.

Proof of Confidentiality

Theorem 1: In the random oracle model, the scheme is IND-CCA2 secure under CDH assumption. Lemmas 1 and 2 have been used to prove the theorem.

Lemma 1: Assuming there exists an adversary A_I who has non-negligible advantage ε of breaking the proposed CLSC scheme, then there exists an algorithm C that can use this adversary to solve the CDH problem with an advantage $Adv_{A_I}{}^{IND-CLSC-CCA2} \geq \frac{\varepsilon}{q_0{}^2 q_2}(1-\frac{1}{(q_2+1)})^{q_s}\frac{1}{(q_s+1)}$, where q_s is signcryption query. The adversary A_I performs q_s queries and q_i hash queries $H_{i(i=0,1,2)}$ to random oracles.

Proof To proof Lemma 1, this research shows how algorithm C who is a challenger, attempts to solve CDH problem by taking random instance (P, aP, bP) as input. In order to determine (abP) from interactions with adversary A_I. C does not know the values of $a, b \in Z_q{}^*$. The challenger C maintains lists L_0, L_1 and L_2 associated with H_0, H_1 and H_2 random oracles respectively and lists L_D, L_{PK} and L_{SK} to track partial private key, public key and private key generation respectively.

Setup: C executes Setup algorithm and sends system params to adversary A_I and simulates partial private key, public key, public key replacement, signcryption and unsigncryption oracle for response to queries from the adversary.

Find stage: Adversary $A_I$issues a number of queries in an adaptive manner and C responds as follows:

$H_0 Queries$: When $A_I$issues random oracle queries on $(ID_i, R_i, P_{pub}, h_0, c)$, C first checks list L_0 for tuple $(ID_i, R_i, P_{pub}, h_0, c)$ which is empty at the start. If it exists, it returns h_0 as an answer. Otherwise, challenger C selects random $c = 0,1$. If $c = 1$ then $Pr[c = 1] =$

$\sigma = 1/(q_s + 1)$ else if $c = 0$ then it selects a random $h_0 \in Z_q{}^*$, returns it to adversary $A_1$and updates list L_0 with tuple $(ID_i, R_i, P_{pub}, h_0, c)$.

$H_1 Queries$: When A_1issues H_1 random oracle queries on tuple $(m, PK_s, \beta, R_r, ID_s, ID_r)$. The challenger C checks whether a matching tuple $(m, PK_s, \beta, R_r, ID_s, ID_r, c_0)$ exists in list L_1which is empty at start, if it exists C returns value c_0 else it returns a random value from $Z_q{}^*$and updates list $L_1$with tuple $(m, PK_s, \beta, R_r, ID_s, ID_r, c_0)$.

$H_2 Queries$: When A_1issues a query on tuple (W, β, R_s, v) C first checks whether there exists a matching tuple (W, β, R_s, v, c_2) in list L_2 which is initially empty. If it exists, it returns symmetric key value c_2 to A_1 else it returns a random value $c_1 \in \{0,1\}^\mu$ and adds tuple (W, β, R_s, v, c_2) to list L_2.

$Partial\ Private\ Key(ID_i)$: If adversary A_1issues a partial private key query on (ID_i, R, P_{pub}). C will check in list L_D for a partial key d_i corresponding to identify ID_i if it exists, it returns value d_i to adversary A_1 else, a random value $r, z \in Z_q{}^*$and obtain d_i by computing $d_i = r + z \cdot H_0(ID_i, R_i, P_{pub})\ mod\ q$ and returns d_i to adversary A_1. The challenger C updates list L_D with tuple $(ID_i, R_i, P_{pub}, d_i)$.

$Private\ Key\ Query(ID_i)$: Using ID_i adversary A_1 issues private key query. C checks whether tuple (ID_i, d, x) exists in the list L_{sk}. If it exists, C will return (d, x) to adversary A_1. Otherwise, C will randomly select $x \in Z_q{}^*$ and obtain d_i by executing a partial private key query. The challenger C updates list L_{sk} with tuple (ID_i, d, x).

$Public\ Key\ Query(ID_i)$: Adversary A_1may perform a public key query for identity ID_i. Challenger C first scans a list L_{pk} to check whether a matching (R_i, PK_i) exists for the ID_i. If it exists, C returns (R_i, PK_i) to adversary A_1. Otherwise, C proceeds to check list L_D and list L_{sk} for records of identity ID_i. If it exists, C picks (R_i, x_i), computes $PK_i = x_i \cdot P$ and returns (R_i, x_i) to adversary A_1 after updating list L_{pk} with tuple (ID_i, R_i, PK_i). Otherwise, C scans list L_0. If $c = 0$, C will run private key query to return

(R_i, PK_i) to adversary A_1 and update list L_{pk} with tuple (ID_i, R_i, PK_i), C picks random values $r_i, x_i \in Z_q{}^*$ then computes $PK_i = x_i \cdot P$ and $R_i = r_i \cdot P$ then adds tuple (ID_i, R_i, PK_i) to L_{pk}, (ID_i, r_i, x_i, c) to L_{rec} and responds to adversary A_I with $(R_i{}^{'}, PK_i{}^{'})$.

$Replace\ Public\ Key\ Query(ID_i, R_i{}^{'}, PK_i{}^{'})$: Adversary A_1 may perform public key replacement query by submitting values $(R_i{}^{'}, PK_i{}^{'})$ of its choice. The challenger C will replace $(R_i{}^{'}, PK_i{}^{'})$ associated with the ID_i with $(R_i{}^{'}, PK_i{}^{'})$.

$Signcryption\ Query(Q_s)$: A_I issues a signcryption query with input (m_i, ID_s, ID_r) where m_i denotes the message, ID_s is the sender's identity and ID_r is the receiver's identity. Challenger C will proceed to check $(ID_s\ , R_s)$ in list L_{pk} for (ID_s, PK_s, R_s) and (ID_r, PK_r, R_r). C will runs actual signcryption algorithm $\psi = (v, c_0, c_1)$ to adversary A_1.

Un$Signcryption\ Query(Q_{us})$: Adversary A_1 may perform an unsigncryption query on ψ sender identity ID_s and receiver identity ID_r. Challenger C will proceed to get (ID_s, PK_s, R_s) from list L_{pk} and (ID_r, d_r, x_r) from list L_{sk} only if c in list $L_0$is $c = 0$ and computes $sx_r = d_r \cdot x_r$. The challenger C will run unsigncryption algorithm and return message m_i to adversary A_I. If $c = 1$, C will check in list L_2 for tuple (Q, β, R_s, v, h_2), compute $m' = D_{h2}(c_1)$ where $h_2 = c_2$ and completes unsigncryption. C will obtain h_1 by calling H_1query. If $h_1 = c_0$ holds message m'_i is returned to adversary A_1 else error $\perp$ is returned.

$\boldsymbol{Challenge\ Phase}$: Adversary A_1 will choose and output two messages m_0 and m_1 of equal length together with sender's ID_s* and receiver's identity ID_r* on which it wishes to be challenged with a few restrictions. Adversary A_I cannot extract the private key for identity ID_r* in find stage, Identity ID_r* is not the identity for which partial private key has been extracted before the challenge and identity ID_r* is not the identity for which the public key has been replaced before the challenge. If $c = 1$, C checks if (x_r, r_r) exists in the list L_{rec} then C will select random values $v^*, c_0^*, c_1^* \in_R Z_q^*$ and sends the challenge ciphertext $\psi *$ to adversary A_I. If $c = 0$, C aborts the process.

Guess Stage: Upon receiving the challenge ciphertext $\psi *$, A_I is allowed to issue a series of queries as was done in Find stage with certain restrictions: If the public key for identity ID_r* has been replaced before the challenge phase the A_I cannot query private key for ID_r*. The adversary cannot make unsigncryption query for $\psi *$ to recover message m_b. A_I returns its guess. The challenger C will ignore the guess from the adversary and select a random entry of tuple $(W^*, \beta^*, R_s, v, c_2)$ in list L_2 and return β^* as the solution to the CDH instance. Otherwise, C is unable to solve CDH problem. The probability that A_I runs private key or partial private for identity ID_r is at least $\frac{1}{q_1^2}$. The probability that C will successfully select $\psi *$ as an answer to CDH is $\frac{1}{q_2}$. The probability that the process will not terminate in phase 1 is $(1-\delta)^{q_s}$ and the probability that it will not terminate in challenge stage is δ. The probability of challenger C not aborting the simulation process is at least $\frac{\varepsilon}{{q_0}^2 q_2}(1-\frac{1}{(q_2+1)})^{q_s}\frac{1}{(q_s+1)}$. A_I can break the confidentiality of the proposed signcryption scheme with a non-negligible advantage ε only if C does not abort the simulation process. It is possible for C to output a solution to CDH problem with advantage ${Adv_{A_I}}^{IND-CLSC-CCA2} \geq \frac{\varepsilon}{{q_0}^2 q_2}(1-\frac{1}{(q_2+1)})^{q_s}\frac{1}{(q_s+1)}$

Lemma 2 Assuming there exists and adversary A_{II} who has non-negligible advantage ε of breaking the proposed CLSC scheme, then there exists and algorithm C that can use this adversary to solve the CDH problem with advantage ${Adv_{A_{II}}}^{IND-CLSC-CCA2} \geq \frac{\varepsilon}{{q_0}^2 q_2}(1-\frac{1}{(q_2+1)})^{q_s}\frac{1}{(q_s+1)}$, where q_s is signcryption query. The adversary A_{II} performs q_s queries and q_i hash queries $H_{i(i=0,1,2)}$ to random oracles.

Proof Challenger C takes as input (P, aP, bP) and attempts to compute (abP) in order to solve CDH problem by utilizing the adversary A_{II} in the game. The proof idea is very similar to the proof of previous lemma except A_{II} cannot issue *Replace Public Key query* . Adversary A_{II} knows the secret key z and goes ahead to set $R = zP$ and inserts $(ID, x, -, c)$ into L_{rec}. In the guess stage, C will output $\beta = x_r \cdot z \cdot P = abP$ as an answer to the CDH problem. The analysis of the game is similar to the proof in Lemma 1.

Proof of Unforgeability

Theorem 2 The proposed scheme is EUF-CMA secure under DLP assumption in the random oracle model.

Lemma 3 Assuming there exists and adversary $A_{i(i=I,II)}$ who can win EUF-CMA game with non-negligible advantage ε, there will be an adversary$C$ that can solve the elliptic curve DL problem with advantage $\frac{\varepsilon}{9_{q2}}(1 - \frac{1}{(q_s+1)})^{q_s}$, where q_s queries to signcryption and the adversary $A_{i(i=I,II)}$ performs q_1 to random oracle $H_{i(i=0,1,2)}$.

Proof Lemma 3 is used to proof theorem 2. C is challenged with an instance of DLP whereby given a random instance $(P, aP) \in G$ its aim is to determine values $(a \in Z_P)$ to achieve (aP). Let adversary $A_{i(i=I,II)}$ be an adversary who can break the EUF-CMA security of the proposed CLSC scheme, algorithm C can utilize $A_{i(i=I,II)}$ to find the solution to aP of ECDLP instance by playing the following interactive game.

Training: Adversary A_I issues a series of queries, where all queries and answers are identical to those in Find stage Lemma 1, whereas the adversary A_{II} issues a series of queries where all queries and answers are identical to those in Lemma 2.

Forgery: At the end of the training the adversary $A_{i(i=I,II)}$ outputs a forgery of tuple $(\psi *$ $,ID_s*,ID_r*)$ from sender ID_s* to receiver ID_r* and the tuple should not have been produced by the signcryption oracle. ID_s* should not be the identity for which partial private key has been extracted and public key replaced. C submit H_1 queries for a random c_0 and retrieves another random $c *_0$ from list L_1 corresponding $(v *, c *_0, c_1)$ such that $c *_0 \neq c_0$. Using forking lemma (Yu et al.,2017) $vP = c_0 \cdot W \cdot T$ and $v^*P = c_0^* \cdot W \cdot T$

is obtained. The two expressions $vP - v^{*}P = c_{0} - c_{0}{}^{*}(W \cdot T)$ are subtracted, given that $T = (b \cdot x_{s})^{-1}$ challenger C utilizes adversary A_{I} as a subroutine to solve

DLP as $b = k(c_{0} - c^{*}{}_{0})/x_{s}(v - v^{*})$ for a given random instance $(P, aP) \in G.$ C utilizes adversary A_{II} to solve DLP as $x = k(c_{0} - c^{*}{}_{0})/d_{s}(v - v^{*})$ for a given random instance $(P, aP) \in G$. The probability that $A_{i(i=I,II)}$runs partial private key queries or private key queries for sender ID_{s} is at least $1/(q^{2}{}_{0})$. The non-termination probability is $(1 - \delta)^{q_s}$ in the training stage. The probability of a failure will be less than $\frac{1}{9}$ when multiple effective ciphertext are produced with replay technique (Yu et al.,2017). The probability that challenger C solves DL problem is at least $1/9q_{2}$ and the probability that C successfully forges a user is at least $\frac{\varepsilon}{9_{q2}}(1 - \frac{1}{(q_{s}+1)})^{q_s}$.

4.6.2 Ubiquitous Healthcare monitoring system

This research showed how the proposed signcryption scheme can be applied in ubiquitous healthcare monitoring system making use of a WBAN where a patient has wearable body sensors that are used to gather physiological data without the interference of the patients daily activities or the presence of a medical expert. A local server which can be a handheld device such as a mobile phone transmits the physiological data to a remote healthcare server via internet. When the data is in the medical server medical personnel can securely access the patient’s data.

The KGC is in charge of generating all the system parameters, partial private key and the public verification tokens. The KGC will run the setup algorithm and generate system parameters then forwards them to the healthcare server and the sensor nodes.

a) **KGC:** Will receive the identity ID_{i} of all the authorized sensor nodes in a WBAN and the identity ID_{i} of the Healthcare server. The Healthcare’s partial private key is computed as $d_{HS_i} = r_{HS_i} + s \cdot H_{0}(ID_{server}, R_{HS_i}, P_{pub})$ mod q and the sensor node partial private key is computed as $d_{S_i} = r_{S_i} + s \cdot H_{0}(ID_{sensor}, R_{S_i}, P_{pub})$

mod q and forwards d_{HS_i} to the healthcare server and d_{S_i} to the sensor node through a secure channel. The KGC will receive public key PK_i from sensor node and computes the public key verification token as $PKV_i = R_i + msk \cdot H_0(ID_{sensor}, PK_i, P_{pub})$ and forwards (ID_i, R_i, PK_i, PKV_i) of each sensor node to the Healthcare server. The KGC will also receive public key PK_i from Healthcare server and computes the public key verification token as $PKV_i = R_i + msk \cdot H_0(ID_{server}, PK_i, P_{pub})$ and forwards (ID_i, R_i, PK_i, PKV_i) to each sensor node in the WBAN.

b) **WBAN:** The validity of the partial private key can be check using the system parameters and computing $d_{S_i} \cdot P = H_0(ID_{sensor}, R_{S_i}, P_{pub}) \cdot P_{pub}$ if the equation does not hold then the process will be terminated else, the node will randomly select $x_i \in Z_p^*$ and compute its public key as $PK_i = d_{s_i} \cdot x_i \cdot P$ then forwards it to the KGC. The wireless sensor node executes the Full private key algorithm and sets the full private key as (d_{s_i}, x_i).

c) **Healthcare Server:** This server will use system parameters provided by KGC to check the validity of the partial private key it received from KGC by computing $d_{HS_i} \cdot P = H_0(ID_{server}, R_{HS_i}, P_{pub}) \cdot P_{pub}$. If the equation holds the healthcare server will randomly select a value $x_i \in Z_p^*$ and compute its public key as $PK_i = d_{Hs_i} \cdot x_i \cdot P$ then forwards it to the KGC. The Healthcare server will set its full private key as (d_{Hs_i}, x_i).

d) **Local Sever:** The local server will be responsible for transmitting data from the sensor to the Healthcare server.

To transmit a patient's physiological values to the Healthcare server, the WBAN client signcrypts a plaintext message m_i by running the signcryption algorithm to output ciphertext $\psi = (v, c_0, c_1)$ and its public key PK_i. The Local Server will act as a controller by transmitting ψ to the Healthcare Server. When the Healthcare Server receives ciphertext ψ, given the public key PK_i is valid it will run the unsigncryption algorithm of the proposed signcryption scheme to recover the original plaintext message m_i'. The validity of m_i' will hold if $c_0' = c_0$ else the plaintext message m_i' will be rejected. A controller can keep a revocation list that stores the identities of all revoked sensor nodes. The revocation process can make use of expiration data which can be denoted as ED. All users are assigned a unique ED set as current date/timestamp during the registration process. Every communication from a user will be concatenated with the ED. The expiration of the ED denies a user access to the WBAN data. A service provider privileged to operate as a KGC can send a revoked user ID_i to the controller if there is an urgent need to revoke a user's access to the WBAN before expiration of the user's ED.

4.6.3 Performance Evaluation

In this research the scheme was evaluated in comparison with the schemes by (Wahid & Mambo, 2016; Won et al., 2015). The scheme was evaluated with respect to computational cost and energy cost. The experiment was implemented on Contiki 2.7 operating system utilizing Cooja simulator to emulate Wismote sensor nodes. The research considered expensive EC operations: modular inverse, point multiplication and point addition operations and denoted as MI, PM and PA respectively.

Table 17: Performance Comparison

Scheme	**Sender**			**Receiver**		
	MI	**PM**	**PA**	**MI**	**PM**	**PA**
Won et al., 2015	0	4	2	0	6	3
Wahid & mambo, 2016	0	3	2	0	5	3
Proposed scheme	1	2	0	1	2	0

Computational Cost

The cryptographic running time for PM, PA and MI are: 4782 ms, 10ms and 577ms respectively. Utilizing the data in Table 17, to generate a ciphertext the scheme by (Won et al., 2015) will require $4PM + 2PA$ and the scheme by (Wahid & Mambo, 2016) will require $3PM + 2PA$ while the proposed scheme $MI + 2PA$. In unsigncryption algorithm the scheme by (Won et al., 2015), (Wahid & Mambo, 2016) and the proposed scheme will require $6PM + 3PA$, $5PM + 3PA$ and $MI + 2PM$ operations respectively. Therefore, the computational time of the schemes by (Won et al., 2015) , (Wahid & Mambo, 2016) and the proposed scheme is $4 * 4782 + 2 * 10 = 19148ms/19.5s$, $3 * 4782 + 2 * 10 = 14366ms/14.37s$ and $577 + 2 * 4782 = 10141ms/10.14s$. It is quite clear that the proposed scheme has the least computational time.

Energy Cost

The performance of the proposed signcryption scheme on Wismote platform is compared to other related signcryption schemes by (Won et al., 2015) and (Wahid & Mambo, 2016). A study by (Dunkel et al.,2007) describes an energy evaluation mechanism on wireless sensor nodes. It makes use of a linear model where the total energy consumption is defined as $\frac{E}{V} = I_m t_m + I_l t_l + I_t t_t + I_r t_r + \Sigma_i I_{c_i} t_{c_i}$, where V represents supply voltage, I_m denotes current draw when the microprocessor has been running. The $I_l t_l$ represents current draw while $I_t t_t$ represents current draw and time of communication device in transmit mode, $I_r t_r$ is the current draw and time of the communication device in receive mode. The current draw and time of components such as sensor nodes and LEDs are represented by $I_{c_i} t_{c_i}$. This research only considered the first four parameters as done in (Nguyen et al., 2015). When running on elliptic curve nist-p224 the estimated energy costs on Wismote for PM, PA and MI are: $32.05mJ$,$0.07mJ$ and $3.81mJ$ respectively. From table 17, the energy consumption for each scheme is as follows:

(a) The scheme proposed by (Won et al., 2015) will require 4*32.05+2*0.07=128mJ to generate a valid ciphertext and it's unsigncryption algorithm will consume 6*32.05+3*0.07=192.5mJ.

(b) The signcryption energy consumption for the scheme by (Wahid & Mambo, 2016) is $3 * 32.05 + 2 * 0.07 = 96.29\, mJ$ while unsigncryption will consume $5 * 32.05 + 3 * 0.07 = 160.46mJ$.

(c) The energy needed to generate a ciphertext in the proposed signcryption scheme is $3.81 + 2 * 32.05 = 67.91mJ$ while unsigncryption will consume $3.81 + 2 * 32.05 = 67.91mJ$.

The proposed signcryption scheme has reduced energy consumption in signcryption as follows:

In the scheme by (Won et al., 2015)$(128.34 - 67.91)/128.34$ =47.1% and in the scheme by (Wahid & Mambo, 2016) (96.29-67.91)/96.29=29%. In the unsigncryption process, the proposed scheme is efficient in energy cost as follows:

In the scheme by (Won et al., 2015)$(192.5 - 67.91)/192.5$ =64.7% while the scheme by (Wahid & Mambo, 2016) the proposed scheme is efficient by $(160.46 - 67.91)/160.46 = 57.7\%.$

4.6.4 Summary

This research has proposed a new pairing free signcryption scheme. Certificateless cryptosystem approach is used in the design of the proposed scheme to overcome key-escrow problem in ID-based schemes and the complexity of certificate management found in PKI. The construction of the scheme is based on the proposed digital signature in subsection 4.2.2. The scheme is secure against adaptive chosen ciphertext attack and against existential forgery. Application area and a network model of the scheme is discussed in (Kasyoka et al., 2021). Further, the proposed signcryption scheme is efficient in computation cost and energy cost as discussed in section 4.6.3.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Contributions

Recent studies have shown that it is possible to implement public key cryptography such as Elliptic Curve Cryptography to resource constrained devices such environments such as WSNs. To address security challenges on WSNs, this thesis has proposed:

1. An efficient digital signature scheme, a variant of ECDSA that can be applied on WSNs to provide authentication. The research showed how the proposed digital signature scheme can be implemented in resource constrained environment through:
    a. A certificateless pairing-free authentication scheme for Wireless Body Area Network for use in healthcare management system. The performance analysis of the proposed scheme was compared with other related schemes and found to be efficient as discussed in section 4.2.4
    b. A Multi-user broadcast authentications scheme for Wireless Sensor Networks. The scheme is certificateless pairing free and has the property of message recovery and ciphertext authenticity. The performance analysis of the cryptographic scheme was compared with other related schemes and found to be more efficient as discussed in section 4.3.5.
2. A Pairing-free certificateless signcryption scheme, a modification of the signcryption scheme by (Wei & Ma, 2019) was proposed in this research. The scheme is existentially unforgeability in Random Oracle Model (ROM) under ECDL problem as discussed in section 4.4.6 and more efficient in both computational cost and energy cost compared to the scheme by (Wei & Ma, 2019) as discussed in section 4.4.7.
3. From the proposed digital signature scheme the research proposed two signcryption schemes. Section 4.5.2 and section 4.6 gives a discuss of the signcryption schemes. The signcryption schemes are secure in IND-CCA2 and

EUF-CMA against Type-I and Type-II attacker in the Random Oracle Model under ECDL problem and CDH problem. The signcryption schemes are efficient in computation cost, energy cost and communication overhead as discussed in sections 4.5.5 and 4.6.3.

5.2 Limitations

In this research two ways to improve efficiency of cryptographic primitives were investigated and a digital signature scheme more efficient in computation compared to the ECDSA was proposed. Signcryption schemes more efficient in computation cost, energy cost and communication cost compared to other related signcryption schemes were also proposed. However, like any other research work, this research had a few limitations:

1. First, this research did not consider transformation of signcryption scheme to online phase and offline phase where heavy complex computations can be performed in offline phase and lightweight computations can be done in online phase. This approach might have improved the efficiency of the proposed signcryption schemes (Saeed et al., 2017).
2. Secondly, this research did not consider heterogenous environments in application of the proposed signcryption schemes.
3. Lastly, the research was limited to simulated environment for testing and application of the proposed signature and signcryption schemes.

5.3 Recommendations

Technological advancements in sensor networks have enable automation and wide range application of WSNs. With wide range application of sensor nodes security has become a major concern and challenge given the inherent resource constraint nature of sensor nodes.

1. Security goal for a resource constrained environment should be identified before designing a cryptographic primitive to support secure communication in such an environment.
2. The design of cryptographic protocols should be efficient enough to support quality communication in the intended application area especially, in Wireless Sensor Networks. This will aid in prolonging the life time of sensor nodes. This

research recommends the use of certificateless and pairing free concepts in the design of cryptographic primitive for use on resource constrained environments.

3. Cryptographic schemes designed must be proved secure in the ROM before they can be adopted for use in an application area.
4. Efficient cryptographic schemes are important for resource constrained environments. However, a well thought out design must be used in the construction of such schemes to ensure proper balance between efficiency and security.
5. This research recommends the adoption and the use of the proposed digital signature/authentication schemes and the signcryption schemes in resource constrained environments such as a WSN.

5.4 Conclusions

The main objective of this research was to develop a signcryption scheme that seeks to ensure efficient and secure communication in resource constrained environment. From the literature it is evident that WSN suffer from insecure communication due to their resource constrained nature. Traditional cryptographic schemes cannot be efficiently applied on WSNs due to their resource constrained nature. hence the need for a computationally efficient but still secure novel cryptosystems.

We conclude that the design of cryptographic protocols should be efficient enough to support quality communication in resource constrained environments. This aids in prolonging the life time of sensor nodes. Existing cryptographic schemes can be modified to withstand stronger attacks and perform more efficiently by reducing computational cost, energy cost and communication overhead. A well designed certificateless and pairing free cryptosystem is more applicable for use on WSNs. However, the security of a WSN should not be compromised over efficiency in communication.

5.5 Future Work

In conclusion this thesis notes that it is possible to have certificateless environment for resource constrained environment and a different cryptographic environment for an application provider especially, where resources used by the application provider are not constrained. The research did not focus on heterogeneous environments and therefore, a possible future work would be application of the proposed signcryption schemes in heterogenous environments. In a heterogeneous environment, entities are allowed to communicate securely using different public cryptographic primitives. The future work on design of heterogeneous signcryption schemes based on the proposed certificateless signcryption schemes would be important to consider. The future work should also seek to utilize the concept of offline/online in the construction of the signcryption schemes as it can improve the overall performance of a signcryption schemes in resource constrained environments.

The application environments used in this research were simulated using software tools and may not have captured an ideal environment scenario. Example, in a healthcare management system where patients wearing a WBAN sensors are being monitored from remote location by healthcare experts as they go about their daily activities. Can the efficiency of the schemes be affected by their daily activities? In future work it would be important to consider implementation in real life.

REFERENCES

Abdullah, K. M., Houssein, E. H., & Zayed, H. H. (2018). New security protocol using hybrid cryptography algorithm for WSN. *International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-6). IEEE.

Abedini , E., & Rezai, A. (2015). A Modified Digital to Digital Encoding Method to Improve the Wireless Body Area Network (WBAN) Transmission. *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)* (pp. 1067-1070). IEEE.

Abidi, B., Jilbab, A., & Mohamed, E. H. (2020). Wireless body area networks: a comprehensive survey. *Journal of Medical Engineering & Technology*. doi: DOI:10.1080/03091902.2020.1729882

Alharbi, K., & Lin, X. (2016). Efficient and privacy-preserving smartgrid downlink communication using identity based signcryption in Global Communications Conference (GLOBECOM). *IEEE*, 1-6.

Ali, M., Sadeghi, M. R., & Liu, X. (2020). Lightweight Fine-Grained Access Control for Wireless Body Area Networks. *Sensors, 20*(4), 1088.

Ali, N. A., Drieberg, M., & Sebastian, P. (2011). Deployment of MICAz mote for wireless sensor network applications. *2011 IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE)* (303-308). IEEE.

Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2016). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal*, 1-10. doi:http://dx.doi.org/10.1016/j.eij.2016.11.001

Alrehily, A. D., Alotaibi, A. F., Almutairy, S. B., Alqhtani, M. S., & Kar, J. (2015). Conventional and improved digital signature scheme: a comparative study. *Journal of information Security, 6*(1), 59.

Al-Riyami, S. S., & Paterson, K. G. (2003). Certificateless public key cryptography. *Adv. Cryptol.-ASIACRYPT*, 452–473.

Al-Shehri, W. (2017). A Survey on Security in Wireless Sensor Networks. *International Journal of Network Security and its Application, 9*(1).

Antipa, A., Brown, D., Gallant, R., Lambert, R., Struik, R., & Vanstone, S. (2006). Accelerated verification of ECDSA signatures. *SAC, 3897*, 307-318.

Anusya, G., Sharmada, M. A., Anitha, G., Akilandeswari, G., & Azees, M. (2018). An Efficient and Secure Authentication Scheme for Wireless Body Area Networks. *2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018)* (pp. 1099-1104). IEEE.

Arfaoui, A., Boudia, O. R., Kribeche, A., Senouci, S. M., & Hamdi, M. (2019). Context-Aware Access Control and Anonymous Authentication in WBANs. *Computers & Security*.

Arunkumar, N., Pandimurugan, V., Hema, M. S., Azath, H., Hariharasitaraman, S., Thilagaraj, M., & Govindan, P. (2022). A Versatile and Ubiquitous IoT-Based Smart Metabolic and Immune Monitoring System. *Computational Intelligence and Neuroscience, 2022*.

Asha, P. N., Mahalakshmi, T., Archana, S., & Lingareddy, S. C. (2016). Wireless Sensor Networks: A Survey on Security Threats Issues and Challenges. *International Journal of Computer Science and Mobile Computing, 5*, 249-267.

Ashraf, S., uddin, N., Sher, M., Ghani, A., & Naqvi, H. (2014). An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography. *Springer Science.*

Barbosa , M., & Farshim,, P. (2008). Certificateless Signcryption. *ACM Symposium on Information Computer and Communication Security (ASIACCS 08).* ACM.

Barekar, P. V., & Hande, K. N. (2012). Performance analysis of timing attack on Elliptic Curve Cryptosystem. *IJCER, 2*(3), 740-743.

Barreto, P. L., Lynn, B., & Scott, M. (2004). Efficient implementation of pairing based crypto systems. *Journal of Cryptology, 17*(14), 321-334.

Barreto, P. L., Libert, B., & McCullagh, N. (2005). Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. *Adv. Cryptol.-ASIACRYPT 2005,* 515–532.

Barreto, P., Deusajute, A. M., Cruz, E., Pereira, G., & Silva, R. (2008). Toward efficient certificateless signcryption from (and without) bilinear pairings. *Preprint*.

Bashirpour, H., Bashirpour, S., Shamshirband, S., & Chronopoulos, A. (2018). An Improved Digital Signature Protocol to Multi-User Broadcast Authentication Based on Elliptic Curve Cryptography in Wireless Sensor Networks (WSNs). *MDPI, 23*(17), 1-15.

Bellare, M. (1997). Practice-oriented provable-security. *International Workshop on Information Security* (pp. 221-231). Springer, Berlin, Heidelberg.

Bellare, M., & Rogaway, P. (1996). The exact security of digital signatures-how to sign with RSA and Rabin. *Advances in Cryptology-EUROCRYPT'96, LNCS 0950,* (pp. 399–416). Ireland.

BenSaleh, M. S., Saida, R., Kacem, Y. H., & Abid, M. (2020). Wireless Sensor Network Design Methodologies: A Survey. *Journal of Sensors, 2020.*

Benzaid, C., Lounis, K., Al-Nemrat, A., Badache, N., & Alazad, M. (2016). Fast authentication in wireless sensor networks. *Future Generation Computer Systems, 55,* 362-375.

Benzaid, C., Medjadba, S., & Badache, N. (2012). Fast Verification of an ID-based Signature Scheme for Broadcast Authentication in Wireless Sensor Networks.

Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. *IEEE Symp. Security Privacy,* (pp. 321-334). Berkeley,C.A, USA.

Bhushan, B., & Sahoo, G. (2019). A Hybrid Secure and Energy Efficient Cluster Based Intrusion Detection system for Wireless Sensing Environment. *2nd International Conference on Signal Processing and Communication (ICSPC),* (pp. 325-329).

Boneh, D., & Franklin, M. (2003). Identity-based encryption from the Weil pairing. *SIAM Journal of Computing, 32,* 586-615.

Bradai, N., Lamia , C., & Lotfi , K. (2011). A comprehensive overview of wireless body area networks (WBAn). *International Journal of E-Health and Medical Communications (IJEHMC), 2*(3), 1-30.

Braun, M., & Kargl, A. (2007). A Note on Signature Standards. *IACR Cryptology ePrint Archive,* 357.

Brown, D. (2001). *The exact security of ECDSA.* Depertment of C& O. University of Waterloo.

Brown, D. L. (2010, January). Standards for Efficient Cryptography Group (SECG). Recommended Elliptic Curve Domain Parameters. *SEC 2*.

Bütün, İ., & Demirer, M. (2013). A blind digital signature scheme using elliptic curve digital signature algorithm. *Turkish Journal of Electrical Engineering & Computer Sciences, 21*(4), 945-956.

Cagalaban, G., & Kim, S. (2011). Towards a secure patient information access control in ubiquitous healthcare systems using identity-based signcryption. *13Th international conference on advanced communication technology (ICACT2011),* (pp. 863–867).

Cao, X., Kou, W., & Du, X. (2010). A Pairing-Free Identity-Based Authenticated Key Agreement Protocol with Minimal. *Inf. Sci, 180,* 2895-2903.

Cao, X., Kou, W., Dang, L., & Zhao, B. (2008). IMBAS: identity-based multiuser broadcast authentication in wireless sensor networks. *Comput. Commun., 31*(4), 659-667.

Chaitra, H. V., & RaviKumar, G. K. (2021). Secure and Energy-Efficient Data Transmission.In Advances in Artificial Intelligence and Data Engineering (pp. 1311-1322). Springer, Singapore.

Chang, S. M., Shieh, S., Lin, W. W., & Hsieh, C. M. (2006). An efficient broadcast authentication scheme in wireless sensor networks. *2006 ACM Symposium on Information, computer and communications security* (pp. 311-320). ACM.

Chatterjee, S., Das, A. K., & Sing, J. K. (2013). A novel and efficient user access control scheme for wireless body area sensor networks. *Journal of King Saud University*. doi:http://dx.doi.org/10.1016/j.jksuci.2013.10.007

Chen, L., & Malone-Lee, J. (2005). Improved identity-based signcryption. In Public key cryptography-PKC. *Berlin: Springer,* 362–379.

Chen-Yang, C., Iuon-Chang, L., & Shu-Yan, H. (2015). An RSA-Like Scheme for Multiuser Broadcast Authentication in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks, 11*(9).

Chien, H. Y., Lee, C. I., & Wu, C. (2013). Comments on IMBAS: identity-based multi-user broadcast authentication in wireless sensor networks. *Security Commun. Networks, 6*, 993-998.

Chipara, O., Lu, C., Bailey, T. C., & Roman, G. C. (2009). *Reliable patient monitoring: A clinical study in a step-down hospital unit.* Washington University at St. Louis, Department of Computer Science and Engineering. Technical Report WUCSE-2009-82.

Choo, K. K. R., Gai, K., Chiaraviglio, L., & Yang, Q. (2020). A Multidisciplinary Approach to Internet of Things (IoT) Cybersecurity and Risk Management.

Chung, F. Y., Huang, K. H., Lai, F., & Chen, T. S. (2007). ID-Based digital signature scheme on elliptic curve cryptosystem. *Comput.Stand. Interfaces, 29*, 601-604.

Costa, D. G., Figueredo, S., & Oliveira, G. (2017). Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions. *Cryptography*.

Cramer, R., & Shoup, V. (1998, August). A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Annual international cryptology conference* (pp. 13-25). Springer, Berlin, Heidelberg

Cramer, R., & Shoup, V. (1999). Signature schemes based on the strong RSA assumption. *7th ACM Conference on Computer and Communications Security* (pp. 46-51). ACM.

Cui, S., Duan, P., Chan, C. W., & Cheng, X. (2007). An Efficient Identity-based Signature Scheme and Its Applications. *IJ Network Security, 5*(1), 89-98.

Debiao, H., Jianhua, C., & Jin, H. (2011). An ID-based proxy signature schemes without bilinear pairings. *Annals of telecommunications-annales des télécommunications*, *66*(11), 657-662.

Dent, A. W. (2006). Fundamental problems in provable security and cryptography. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 364*(1849), 3215-3230.

Dharminder, D., & Mishra, D. (2020). Understanding signcryption security in the standard model. *Security and Privacy, 3*(3).

Diffie, W., & Hellman, M. E. (1976, November). New directions in cryptography. *IEEE Trans Inform. Theory*.

Dindayal, M., & Dilip, K. Y. (2017). RSA and ECC: A Comparative Analysis. *International Journal of Applied Engineering Research, 12*(19), 053-9061.

Dunkels, A., Gronvall, B., & Voigt, T. (2004). A Lightweight and flexible operating system for tiny networked sensors. *Proceedings of the First IEEE Workshop on Embedded Networked Sensors*. Tampa, Florida.

Dunkels, A., Grovall, B., & Voigt, T. (2004). Contiki-a lightweight and flexible operating system for tiny networked sensors. *29th Annual IEEE International Conference on Local Computer Networks* (pp. 455-462). IEEE.

Dunkels, A., Osterlind, F., Tsiftes, N., & He, Z. (2007, June). Software-based on-line energy estimation for sensor nodes. In *Proceedings of the 4th workshop on Embedded networked sensors* (pp. 28-32).

Dutta, M., Singh, A. K., & Kumar, A. (2013, February). An efficient signcryption scheme based on ECC with forward secrecy and encrypted message authentication. In *2013 3rd IEEE International Advance Computing Conference (IACC)* (pp. 399-403). IEEE.

Dutta, R., Barua, R., & Sarkar, P. (2004). Pairing-Based Cryptographic Protocols: A Survey. *IACR Cryptology ePrint Archive*, 64.

Easttom, W. (2021). Cryptographic Hashes. In *Modern Cryptography* (pp. 205-224). Springer, Cham.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, *31*(4), 469-472.

ELkamchouchi, H. M., Elkeheir, E. F., & Aboue, Y. (2014). An Improved Authentication Protocol for Mobile Communication based on Tripartite Signcryption. *Internation Journal of Computer Applications*, *92*(14).

Enos, G., & Zheng, Y. (2015). An ID-based signcryption scheme with compartmented secret sharing for unsigncryption. *Elsever*, 128-133.

Fagen, L., & Xiong, P. (2013). Practical Secure Communication for Integrating Wireless Sensor Networks into the Internet of Things. *IEEE*, *13*(10), 3677-3684.

Fang, W., Wen, X., Xu, J., & Zhu, J. (2019). CSDA: a novel cluster-based secure data aggregation scheme for WSNs. Cluster Computing, 22(3), 5233-5244.

Fang, X., Yang, G., & Wu, Y. (2017). Research on the underlying method of elliptic curve cryptography. *4th International Conference on Information Science and Control Engineering.* IEEE.

Faquih, A., Kadam, P., & Saqui, Z. (2015). Cryptographic Techniques for Wireless Sensor Networks: Survey. *IEEE*.

Farahmandian, M., Masdari, M., & Farahmandian, V. (2014). Comprehensive Analysis of Broadcast Authentication protocols in Wireless Sensor Networks. *Journal of Computer Science and Information Technology*, *2*(3), 107-125.

Freeman, D., Scott, M., & Teske, E. (2010, April). A taxonomy of pairing-friendly elliptic curves," Journal of Cryptology. *23*(2), 224–280.

Gao, G. M., Peng, X. G., & Jin, L. Z. (2019). Efficient Access Control Scheme with Certificateless Signcryption for Wireless Body Area Networks. *International Journal of Network Security, 21*(3), 428-437.

Gayathri, N. B., T, G., R.R.V, K. R., & Vasudeva, R. (2018). Efficient and Secure pairing-free certificateless directed signature scheme. *Journal of King Saud University-Computer and Information Sciences*.

Genç, Y., & Afacan, E. (2021, April). Design and implementation of an efficient elliptic curve digital signature algorithm (ECDSA). In *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)* (pp. 1-6). IEEE.

Ghani, A., Mansoor, K., Mehmood, S., Chaudhry, S. A., Rahman, A. U., & Najmus, S. M. (2019). Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key. *International Journal of Communication Systems, 32*(16), e4139.

Goldreich, O. (1999). Modern Cryptography, Probabilistic Proofs and Pseudorandomness. *SpringerVerlag*.

Gonzalez, M. L., Gayoso, M. V., & Martin, M. A. (2018). Secure elliptic curves in cryptography. *Computer and Network Security Essenstials*. doi:https://doi.org/10.1007/978-3-319-58424-9_16

Grover, K., & Lim, A. (2015). A survey of broadcast authentication schemes for wireless networks. *Ad Hoc Networks, 24*, 288-316.

Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (2004). Comparing Elliptic curve cryptography and RSA on 8-bit CPUs. *Cryptographic Hardware and Embedded Systems, 3156*, 119-132.

Hamdy, W., Al-Awamry, A., & Mostafa, N. (2022). Warehousing 4.0: A proposed system of using node-red for applying internet of things in warehousing. *Sustainable Futures*, *4*, 100069.

Han, W. (2011). Weakness of a Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. *IACR*.

He, D., & Zeadally, S. (2015). Authentication protocol for an ambient assisted living system. *IEEE Commun. Mag.*, *53*(1), 71-77.

He, D., Zeadally, S., & Neeraj, K. (2017). Anonymous Authentication for Wireless Body Area Networks With Provable Security. *IEEE Systems Journal*, *11*(4), 2590-2601.

Hou, X., Wang, J., Jiang, C., Guan, S., & Ren, Y. (2018, May). A sink node assisted lightweight intrusion detection mechanism for WBAN. In *2018 IEEE International Conference on Communications (ICC)* (1-6). IEEE

Hu, C., Li, H., Huo, Y., Xiang, T., & Liao, C. (2016). Secure and efficient data communication protocol for wireless body. *Multi-Scale Comput. Syst, 2*(2), 94-107.

Hu, C., Zhang, F., Cheng, X., Liao, X., & Chen, D. (2013). Securing communications between external users and wireless body area networks. *2nd ACM Workshop Hot Topics Wireless Netw. Security Privacy*, (31-35). Budapest, Hungary.

Hu, X., & Zhiguang , Q. (2015). Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. *IEEE Transactions on Information Forensics and Security* , *10*(7), 1442-1455.

Huang, Y., & Yang, J. (2017). A Novel Identity-Based Signcryption Scheme in the Standard Model. *Information, 8*(2), 58.

Huifang, Y., & Bo, Y. (2016). Pairing-Free and Secure Certificateless Signcryption Scheme. *The Computer Journal, 60*(8), 1187-1196.

Hwang, R., Lai, C., & Su, F. (2005). .An efficient signcryption scheme with forward secrecy based on elliptic curve. *Journal of Applied Mathematics and Computation, 167*(2), 870 – 881.

Iqbal, J., Umar, A. I., Amin, N., & Waheed, A. (2019). Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain. *International Journal of Distributed Sensor Networks*, 1550147719875654.

Islam, S. H., Farash, M. S., Biswas, G. P., Khan, M. K., & Obaidat, M. S. (2013). Provably secure and pairing-free certificateless digital multisignature scheme using elliptic curve cryptography. *International Journal of Computer Mathematics, 90*(11), 2244–2258.

Islam, S., & Biswas, G. (2011). A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. *J. Syst. Softw, 84*(11), 1892-1898.

Izza, S., Benssalah, M., & Ouchikh, R. (2018). Security Improvement of the Enhanced 1-round Authentication Protocol for Wireless Body Area Networks. *2018 International Conference on Applied Smart Systems (ICASS'2018).* Medea Algeria: IEEE.

Jebri, S., Abid, M., & Bouallegue, A. (2018). LTAMA-Algorithm: Light and Trust Anonymous Mutual Authentication Algorithm for IoT. *IEEE 87th Vehicular Technology Conference (VTC Spring)* .

Jian, S., Shaohua, C., Jun, S., Qi, L., & Xingming, S. (2016). A lightweight multi-layer authentication protocol for wireless body area networks. *Future Generation Computer Systems*. doi:DOI:http://dx.doi.org/10.1016/j.future.2016.11.033

Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *International journal of information security, 1*(1), 36-63.

Kardi, A., Rachid, Z., & Mohammed, A. (2018). Performance Evaluation of RSA and Elliptic Curve Cryptography in Wireless Sensor Networks. *21st Saudi Computer Society National Computer Conference (NCC).* IEEE.

Karthikeyan, S., Nishanth, A., Praveen, A., & Ravi, T. (2022). Manual and Automatic Control of Appliances Based on Integration of WSN and IOT Technology. In *Mobile Radio Communications and 5G Networks* (1-20). Springer, Singapore

Kasyoka, P. N., Kimwele, M., & Mbandu, S. A. (2021). Efficient certificateless signcryption scheme for wireless sensor networks in ubiquitous healthcare systems. *Wireless Personal Communications, 118*(4), 3349-3366.

Kasyoka, P., Kimwele, M., & Mbandu, A. S. (2020). Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system. *Journal of Medical Engineering & Technology, 44*(1), 12-19.

Kerry, C. F. (2013). Digital signature standard (DSS). *National Institute of Standards and Technology*.

Khaled, A. W. (2019). A Survey on Elliptic Curves Cryptosystems. *Journal of Advanced Research in Dynamical & Control Systems, 11*(1).

Khalilian, R., Abdalhossein, R., & Ehsan, A. (2014). An Efficient Method to Improve WBAN Security. *Advanced Science and Technology Letters, 64*, 43-46. doi:http://dx.doi.org/10.14257/astl.2014.64.11

Khalilian, R., Rezai, A., & Mesrinejad, F. (2016). Secure Wireless Body Area Network(WBAN) Communication Method Using New Random Key Management Scheme. *International Journal of Security and Its Application, 10*(11), 13-22.

Khan, R. A., & Pathan, A.-S. K. (2018). The state-of-the-art wireless body area sensor networks: A survey. *International Journal of Distributed Sensor Networks, 14*(4).

Kheradmand, B. (2013). Enhancing Energy Efficiency in Wireless SensorNetworks via Improving Elliptic Curve Digital Signature Algorithm. *World Applied Sciences Journal, 21*(11), 1616-1620. doi:DOI: 10.5829/idosi.wasj.2013.21.11.166

Kobiltz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation* (48), 203-209.

Koblitz, N. (1994). *A course in number theory and cryptography* (Vol. 114). Springer Science & Business Media.

Koblitz, N., & Menezes, A. J. (2015). The random oracle model: a twenty-year retrospective. *Designs, Codes and Cryptography, 77*(2-3), 587-610.

Koblitz, N., Menezes, A., & Vanstone, S. (2000). The State of Elliptic Curve Cryptography. *Des. Code Cryptogr, 19,* 173-193.

Kothmayr, T., Schmitt, C., Hu, W., Brunig, M., & Carle, G. (2012). A DTLS based end-to-end security architecture for the internet of things with two-way authentication. *Local Computer Networks Workshops (LCN Workshops)* (956-963). IEEE.

Kurosawa, K., & Desmedt, Y. (2004). A new paradigm of hybrid encryption scheme. *Springer*, 456-442.

Lee, J.; Lee, S.; Kim, J.; Oh, H.(2020). Scalable Wildcarded Identity-Based Encryption with Full Security. *Electronics, 9,* 1453.

Li, F. G., Han, Y. Y., & Jin, C. H. (2016). Practical Access Control for Sensor networks in the context of Internet of Things. *Computer Communications*, 154-164.

Li, F., & Hong, J. (2016). Efficient Certificateless Access Control for Wireless Body Area Networks. *Sensor Journal, 16*(13), 5389-5396.

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

Li, F., Hong, J., & Andrew , A. O. (2016). Efficient certificateless access control for industrial Internet of Things. *Future Generation Computer Systems, 76,* 285-292. doi:http://dx.doi.org/10.1016/j.future.2016.12.036

Li, F., Shirase, M., & Takagi, T. (2013). Certificateless hybrid signcryption. *Math. Comput. Model*(57), 324–343.

Li, M., Lou , W., & Kui, R. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless Communication, 17*(1), 51-58.

Liu , J., Zhang, Z., Chen , X., & Kwak , K. S. (2014). Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks. *IEEE Transactions on Parallel and Distributed Systems, 25*(2), 332–342. doi:doi:10.1109/TPDS.2013.145

Liu, J., Zhang, Z., Chen, X., & Kwak, K. S. (2014). Certificateless remote anonymous authentication scheme for wireless body arean networks. *IEEE Trans. Parallel Distrid. Syst., 25*(2), 332-342.

Liu, Z., Hu, Y., Zhang, X., & Ma, H. (2010). Certificate-less signcryption scheme in the standard model. *Information Sciences,* 452-464.

Luo, M., Luo, Y., Wan, Y., & Wang, Z. (2018). Secure and efficient access control scheme for Wireless Sensor Networks in the Cross-Domain Context of the IoT. *Secur. Commun. Netw., 2018,* 1-10. doi:https://doi.org/10.1155/2018/6140978

Lynch, J. P., & Kenneth, J. L. (2006). A Summary Review of Wireless Sensors and Sensor Networks for Structural Health Monitoring. *Shock and Vibration Digest, 38*(2), 91-130.

Ma, C., Xue, K., & Hong, P. (2014). Distributed access control with adaptive privacy preserving property for wireless sensor networks. *Security and Communication Networks , 7*(4), 759–773.

Maidhili, S. R., & Karthik, G. M. (2018). Energy Efficient and Secure Multi-User Broadcast Authentication Scheme in Wireless Sensor Networks. *International Conference On Computer Communication and Informatics (ICCCI-2018).* IEEE.

Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin, J. C. W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors, 22*(6), 2087.

Mandal, M., Sharma, G., & Verma, A. K. (2016). A Computational Review of Identity-based Signcryption Schemes. *International Journal of Network Security, 18*(5), 969-977.

Manju, V. C., Lekha, S. L.,&Kumar, M. S.(2013). Mechanisms for detecting and preventing denial of sleep attacks on wireless sensor networks. *IEEE Conference on Information & Communication Technologies,* Thuckalay, Tamil Nadu, India, pp. 74-77, doi: 10.1109/CICT.2013.6558065.

Mansoor, K., Ghani, A., Chaudhry, S. A., Shamshirband, S., Ghayyur, S. A., & Mosavi, A. (2019). Securing IoT-Based RFID Systems: A Robust Authentication Protocol Using Symmetric Cryptography. *Sensors, 19*(21), 4752.

Mathew, P., Jilna, P., & Deepthi, P. P. (2015). Efficient Implementation of EC based Key Management Scheme on FPGA for WSN. *IEEE.*

Mbarek, B., Meddeb, A., Jaballah, W. B., & Mosbah, M. (2017, January). An efficient Broadcast Authentication Scheme in Wireless Sensor Networks. *ANT/SEIT*, 553-559.

Miller, V. (1985). “Uses of elliptic curves in cryptography-Lecture Notes in Computer Science. *Advances in Cryptology-Crypto ’85*.

Mkongwa, K. G., Liu, Q., Zhang, C., & Siddiqui, F. A. (2019). Reliability and Quality of Service Issues in Wireless Body Area Networks: A Survey. *International Journal of Signal Processing Systems, 7*(1), 26-31. doi:doi: 10.18178/ijsps.7.1.26-31

Mohamed, N. N., Yussoff, Y. M., Saleh, M. A., & Hashim, H. (2020). Hybrid Cryptographic Approach For Internet Ofthings and Applications: A REVIEW. *Journal of Information and Communication Technology, 19*(3), 279-319.

Moon, A. H., Iqbal, U., & Bhat, G. M. (2016). Mutual Entity Authentication Protocol Based on ECDSA for WSN. *Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016).* Elsevier.

Mukherjee, P., & Mukherjee, A. (2019). Advanced processing techniques and secure architecture for sensor networks in ubiquitous healthcare systems. In *Sensors for health monitoring* (3-29). Academic Press.

Narwal, B., & Mohapatra, A. K. (2020). SEEMAKA: Secured Energy-Efficient Mutual Authentication and Key Agreement Scheme for Wireless Body Area Networks. *Wireless Personal Communication*, 1-24.

Narwal, B., & Mohapatra, A. K. (2021). SALMAKA: secured, anonymity preserving and lightweight mutual authentication and key agreement scheme for WBAN. *International Journal of Sensors Wireless Communications and Control*, *11*(4), 374-384.

Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication. *Ad-Hoc Networks journal*. doi:http://dx.doi.org/10.1016/j.adhoc.2015.01.006.

Nguyen, K. T., Oualha , N., & Laurent, M. (2015). Lightweight certificateless and provably secure signcryptosystem for the internet of things. *TRUSTCOM 2015:14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications.*

Nyberg, K., & Rueppel, R. A. (1994, May). Message recovery for signature schemes based on the discrete logarithm problem. In *Workshop on the Theory and Application of of Cryptographic Techniques* (182-193). Springer, Berlin, Heidelberg.

Omala, A. A., Kibiwott, K. P., & Li, F. (2017). An efficient remote authentication scheme for wireless body area network. *Journal of medical systems*, *41*(2), 1-9

Omala, A. A., Mbandu, A. S., Muturi, K. D., & Jin, C. (2018). Provably Secure Heterogeneous Access Control Scheme for Wireless Body Area Network. *J. Med. Syst, 41*(108).

Patil, S. D., & Vijayakumar, B. P. (2016). Overview of Issues and Challenges in Wireless Sensor Networks. *International Journal of Applied or Innovation in Engineering and Management, 5*(5).

Pawar, R., & Kalbande, D. R. (2019). Elliptical Curve Cryptography Based Access Control Solution for IoT Based WSN. *International Conference on Innovative Data Communication Technologies and Application* (742-749). Springer Cham.

Pointcheval, D., & Stern, J. (2000). Security arguments for digital signatures and blind signatures. *Journal of Cryptology, 13*, 361–396.

Pointchevel, D., Stern, J., Malone-Lee, J., & Smart, N. P. (2002). Flaws in Security Proofs. *CRYPTO*.

Prasithsangaree, P., & Krishnamurthy, P. (2004). On a framework for energy-efficient security protocols in wireless networks. *Computer Communications, 27*(17), 1716-1729.

Puttmann, C., Shokrollahi, J., Porrmann, M., & Ruckert, U. (2008). Hardware Accelerators for Elliptic Curve Cryptography. *Advances in Radio Science*, 259-264.

Ramadan, M., Liao, Y., Li, F., Zhou, S., & Abdalla, H. (2020). IBEET-RSA: Identity-based encryption with equality test over RSA for wireless body area networks. *Mobile Networks and Applications, 25*(1), 223-233.

Rezaei, Z., & Mobininejad, S. (2012). Energy Saving In Wireless Sensor Networks. *International Journal of Computer Science and Engineering*.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and publickey cryptosystems. *Communications of the ACM, 21*(2), 120-126.

Saeed, M. E., Liu, Q., Tian, G., Gao, B., & Li, F. (2017). HOOSC: heterogeneous online/offline signcryption for the internet of things. Wireless Networks. doi:DOI 10.1007/s11276-017-1524-z.

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.

Salome, J., N.B, G., & Vasudeva, R. (2018). Pairing-free Identity Based Blind Signature Scheme with Message Recovery. *Cryptography-MDPI, 2*(29).

Saravanakumar, G., Devi, T. M., Karthikeyan, N., & Samuel, B. J. (2021). Secure medical data transmission for DT-WBAN in military environment. *Materials Today: Proceedings*.

Sarath, G., Jinwala, D. C., & Patel, S. (2014). A survey on elliptic curve digital signature algorithm and its variants. *Computer Science & Information Technology (CS & IT)–CSCP*, 121-136.

SEC2. (2000, September). Recommended Elliptic Curve Domain Parameters. *Standards for Efficient Cryptography Group*. Retrieved from http://www.secg.org

Seo, S., & Bertino, E. (2013). Elliptic Curve Cryptography Based Certificateless Hybrid Signcryption Scheme without Pairing. *CERIAS TR 2013-10:CERIAS.* West Lafayette, USA.

Schnorr, C. P. (1989, August). Efficient identification and signatures for smart cards. In *Conference on the Theory and Application of Cryptology* (239-252). Springer, New York, NY.

Shaikh, R. A. J., Naidu, H., & Kokate, P. A. (2021). Next-generation wsn for environmental monitoring employing big data analytics, machine learning and artificial intelligence. In Evolutionary computing and mobile sustainable networks (pp. 181-196). Springer, Singapore.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In Workshop on the. *Workshop on the Theory and Application of Cryptographic Techniques* (47-53). Springer.

Shim, K. A. (2017). Comments on" A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs" by Biswas and Mišić. *IEEE Transactions on Vehicular Technology*, *66*(11), 10588-10589.

Shamshirband, S., Joloudari, J. H., GhasemiGol, M., Saadatfar, H., & Mosavi, A. N. (2020). FCS-MBFLEACH: Designing and Energy-Aware Fault Detection System for Mobile Wireless Sensor Networks. *Mathematics*, *8*(1), 28.

Shao, Z., & Gao, Y. (2014). A provable secure signature scheme based on factoring and discrete logarithms. *Applied Mathematics and Information Sciences, 8*(4), 1553-1558.

Sharma, D., & Singh, J. (2022). A Comparative Analysis of Healthcare Monitoring Systems Using WSN. *ECS Transactions*, *107*(1), 8695.

Sharma, G., Bala, S., & Verma, A. K. (n.d.). An identity-based ring signcryption scheme. *IT convergence and security 2012* (151–157). Springe.

Shen, J., Chang, S., Shen, J., Liu, Q., & Sun, X. (2018). A lightweight multi-layer authentication protocol for wireless body area networks. *Future Gener. Comput. Syst., 78*, 956–963.

Shim , K.-A., Lee , Y.-R., & Park, C.-M. (2013). EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks. *Ad-Hoc Networks, 11*, 182-189. doi:http://dx.doi.org/10.1016/j.adhoc.2012.04.015

Shim, K. A. (2014). S2DRP Secure implementations of distributed reprogramming. *Ad Hoc Netw, 19*, 1-8.

Shim, K.-A. (2007, January). BASIS: A practical Multi-User Broadcast Authentication Scheme in Wireless Sensor Networks. *Information Forensics and Security, 6*(1). doi:DOI 10.1109/TIFS.2017.2668062

Shoup, V. (2004). Sequences of games: a tool for taming complexity in security proofs. *cryptology eprint archive*.

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*, 102499.

Singh, A. K., & Vaisla, K. S. (2014). A lightweight Signcryption Scheme based on Elliptic Curve Cryptography. *First International Conference on* Advances in computing & Communication Engineering (ICACCE).

Singha, A., Mumenin, N., Akhter, N. I., Moon, M., Hossain, S., & Ahmed, M. U. (2022). A Lightweight Cryptographic Scheme to Secure WSNs in Agriculture. In Proceedings of Trends in Electronics and Health Informatics (615-624). Springer, Singapore.

Sivasundari, A., & Ramakrishnan, M. (2019). Hybrid aggregated signcryption scheme using multi-constraints differential evolution algorithm for security. *Cluster Computing, 22*(2), 3201-3211.

Subhas, C. S., Manik, L. D., & Bubu , B. (2019). A provable secure key escrow free identity based signature scheme without using secure channel at the phase of private key issuance. *Indian Academy of Sciences, 44*(12), 1-9.

Sukanya, M., Sindhu, K. V., Gowri, G., & Nandhini, S. G. (2017). Trustworthy access control for wireless body area networks. *2017 International Conference on Information Communication and Embedded Systems (ICICES)* (1-5). IEEE.

Sun, D., Huang, D., & Mu, X. (2008). Identity-based on-line,off-line signcryption. *IFIP international conference on network and parallel computing, 2008*, (34-41).

Tan, C. C., Wang, H., Zhong, S., & Li, Q. (2009). IBE-Lite: A lightweight identity-based cryptography for body sensor networks. *IEEE Trans.Inform. Technol. Biomed, 13*(6), 926-932.

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

Toorani, M., & Baheshti, A. (2009). A directly public verifiable signcryption scheme based on elliptic curves. *In Computers and Communications, 2009. ISCC 2009* (713-716). IEEE Symposium.

Toorani, M., & Shirazi, A. B. (2008). Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve. *In Proceedings of International Conference on Computer and Electrical Engineering (ICCEE'08)*, (428-432).

Ullah, I., Amin, N. U., Khan, M. A., Khattak, H., & Kumari, S. (2021). An Efficient and Provable Secure Certificate-Based Combined Signature, Encryption and Signcryption Scheme for Internet of Things (IoT) in Mobile Health (M-Health) System. *Journal of Medical Systems, 45*(1), 1-14.

Ullah , I., Alomari, A., Ul Amin, N., Khan, M. A., & Khattak, H. (2019). An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the Internet of Things. *Electronics,, 8*(10), 1171.

Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., . . . Kwak, K. S. (2012). A comprehensive survey of wireless body area networks. *Journal of medical systems, 36*(3), 1065-1094.

Upreti, K., Kumar, V., Pal, D., Alam, M. S., & Sharma, A. K. (2022). Design and Development of Tracking System in Communication for Wireless Networking. In *Intelligent Sustainable Systems* (pp. 215-226). Springer, Singapore.

Vaniprabha, A., & Poongodi, P. (2017). Augmented lightweight security scheme with access control model for wireless medical sensor networks. *Cluster Computing, 22*(5), 12495-12505.

Vanstone, S. (1992). Responses to NISTs Proposal. *Communications of the ACM*.

Venkataraman, K., & Sadasivam, T. (2019). FPGA Implementation of Modified Elliptic Curve Digital Signature Algorithm. *Facta Universitatis, Series: Electronics and Energetics, 32*(1), 129-145.

Venkataraman, K., & Sadasivam, T. (2019). FPQA implementation of modified Elliptic Curve Digital Signature Algorithm. *Facta universitatis-series: Electronics and Energetics, 32*(1), 129-145.

Wahid, A., & Mambo, M. (2016). Implementation of Certificateless Signcryption based on Elliptic Curve Using Javascript. International Journal of Computing and Informatics (IJCANDI). *1*(13), 90-100.

Wander, , A., Gura, N., Eberle, H., Gupta, V., & Shantz, S. (2005). Energy analysis of public-key cryptography on small wireless devices. *PerCom'05* (324–328). IEEE.

Wang, C., Jiang, C., Liu, Y., Li, Y. X., & Tang, S. (2014). Aggregation capacity of wireless sensor networks: Extended network case. *63*, pp. 1351-1364. IEEE Transcactions on Computers.

Wei, L., & Ma, W. (2019). Secure and Efficient Data Sharing Scheme Based on Certificateless Hybrid Signcryption for Cloud Storage. *MDPI-Electronics, 8*(590). doi:doi:10.3390/electronics8050590

Winkler, T., & Rinner, B. (2014). Security and Privacy Protection in Visual Sensor Networks. *ACM Computer Survey, 47*, 97-116.

Won, J., Seo, H., & Bertino, E. (2015). A Secure Communication Protocol for Drones and Smart Objects. *ASIA CCS0 2015*, (pp. 249-260).

Xu, J., Wang, K., Wang, Hu, F., Zhang, Z., Xu, S., & Wu, J. (2015). Byzantine fault-tolerant routing for large-scale wireless sensor networks based on fast ECDSA. *Tsinghua Science and Technology, 20*(6), 627-633.

Yu, G., Yang, H., Fan, S., Shen, Y., & Han, W. (2011). Efficient certificateless signcryption scheme from Weil pairing. *Journal of Networks, 6*(9), 1280.

Yu, H. F., & Yang, B. (2017). Low-computation certificateless hybrid signcryption scheme. *Frontiers of Information Technology & Electronic Engineering*, 928-940.

Yuan, Y. (2020). Security Analysis of an Enhanced Certificateless Signcryption in the Standard Model. *Wireless Pers Commun, 112*, 387–394. doi:https://doi.org/10.1007/s11277-020-07031-9

Zhang, L., Wang, P., Zhang, Y., Chi, Z., Tong, N., Wang, L., & Li, F. (2022). An adaptive and robust secret key extraction scheme from high noise wireless channel in IIoT. *Digital Communications and Networks*.

Zhang, Q., Li, Z., & Song, C. (2011). The Improvement of digital signature algorithm Based on elliptic curve cryptography. *IEEE*.

Zheng, Y. (1997). Digital signcryption or how to achieve cost (signature and encryption In Advances in Cryptology CRYPTO '97. *Springer-Verlag, 1294 of Lecture Note in Computer Science*, 165–179.

Zhong, H., Zhao, R., Cui, J., Jiang, X., & Gao, J. (2016). An Improved ECDSA Scheme for Wireless Sensor Network. *International Journal of Future Generation Communication and Networking, 9*, 73-82.

Zhou, Z., & Huang, D. (2010). On efficient ciphertext-policy attribute based encryption and broadcast encryption. *17th ACM conference on Computer and communications security*. Chicago, IL, USA.

Zou, S., Xu, Y., Wang, H., Li, Z., Chen, S., & Hu, B. (2017). A Survey on Secure Wireless Body Area Networks. *Security and Communication Networks*.

LIST OF APPENDICES

Appendix I: Author’s Publications during PhD Study

1. Kasyoka, P., Kimwele, M., & Angolo, S. M. (2021). Cryptanalysis of a Pairing free Certificateless Signcryption scheme. *ICT Express*, *7*(2), 200-204.
2. Kasyoka, P. N., Kimwele, M., & Mbandu, S. A. (2021). Efficient certificateless signcryption scheme for wireless sensor networks in ubiquitous healthcare systems. *Wireless Personal Communications*, *118*(4), 3349-3366.
3. Kasyoka, P., Kimwele, M., & Mbandu Angolo, S. (2020). Certificateless pairing free authentication scheme for wireless body area network in healthcare management system. *Journal of medical engineering & technology*, *44*(1), 12-19.
4. Kasyoka, P., Kimwele, M., & Angolo, S. M. (2020). Towards an efficient certificateless access control scheme for wireless body area networks. *Wireless Personal Communications*, *115*(2), 1257-1275.
5. Kasyoka, P., Kimwele, M., & Angolo, S. M. (2020). Multiuser broadcast authentication scheme for wireless sensor network based on elliptic curve cryptography. *Engineering Reports*, *2*(7), e12176.