DEMOCRATIC And POPULAR REPUBLIC OF ALGERIA
MINISTRY OF HIGH STUDIES AND SCIENTIFIC RESEARCH
UNIVERSITY OF MOHAMED BOUDIAF - M'SILA

MATHEMATICS AND COMPUTER
FACULTY: Mathematics and Informatics
DEPARTEMENT of computer science
N° : …….

DOMAIN: Mathematics and Informatics
BRANCH: Computer Science
OPTION: RTIC

A Dissertation in Fulfillment
For the Requirement of the Degree of MASTER
By:

LAGUEAGUE SIF ELISLAM

CHEIKHAOUI NAIMA

Subject:

LIGHTWEGHT AUTHENTICATION SCHEME FOR PATIENT MONITORING BASED ON POST-QUANTUM CRYPTOGRAPHY

Defended to the jury:

Attir Azzedine	Université de M'sila	Chairman
Chicouche Noureddine	Université de M'sila	Supervisor
Bahache Mohamed	Université de M'sila	Examiner

Academic year: 2021/2022

Dedication

This modest work is dedicated firstly to my beloved parents, who have been a source of inspiration and support Allover and throughout my entire life, thank you for everything that you have done for me. To my Grandparents and specially my Grandfather. To my Brothers and sisters. And to my real friends who have been always to my shoulders.

AKNOWLEGEMENT

First of all , I'll Say Al hamdolillah , I thank Allah for such blessing , and that he gave me strength and ability to complete this dissertation .

I'll express my deepest gratitude to my advisor

Mr **Chicouche Noureddine** *for his guidance and support throughout the study, I also thank Mr Bahache Anwar for also guiding and supporting me. I'll thank my colleges and friends that shared their experiences and knowledge*

Finally, I am deeply grateful to my parents for their trust everlasting love, care, and indefectible support during all my years of studying.

Abstract

The Wireless Body Area Network (WBAN) is one of the promising wireless sensor technologies that improve healthcare and constantly exchange health information during authentic time. However, in such a novel system paradigm, a require of a clearly-defined defense line would cause potential users to be concerned about the reveal of their personal information, especially for unauthorized or level malevolent opponents. This dissertation describes an efficient and lightweight authentication scheme base on post quantum cryptography method for protecting the patient's medicinal information in WBAN. This method uses the asymmetric encryption algorithm toward encrypt otherwise decrypt the secret data, and the key to establish that was the KYBER with IND-CPA level encryption scheme.

Keywords: Post-quantum cryptography, authentication protocol, security, WBAN.

Résumé :

Les réseaux corporel sans fil (WBAN) est l'une des technologies de capteurs sans fil prometteuses qui améliorent les soins de santé et échangent constamment des informations sur la santé en temps réel. Cependant, dans un tel nouveau paradigme de système, l'exigence d'une ligne de défense clairement définie amènerait les utilisateurs potentiels à s'inquiéter de la révélation de leurs informations personnelles, en particulier pour les adversaires malveillants non autorisés ou de niveau. Cette thèse décrit un schéma d'authentification efficace et léger basé sur la méthode de cryptographie post-quantique pour protéger les informations médicales du patient dans WBAN. Cette méthode utilise l'algorithme de cryptage asymétrique pour crypter et décrypter les données secrètes, et la génération de clés pour établir qui était le schéma de cryptage KYBER de niveau IND-CPA.

Mots clés : cryptographie post-quantum, protocole d'authentification, sécurité, WBAN.

الملخص:

تعد شبكة منطقة الجسم اللاسلكية (WBAN) إحدى تقنيات الاستشعار اللاسلكية الواعدة التي تعمل على تحسين الرعاية الصحية وتبادل المعلومات الصحية باستمرار خلال الوقت الحقيقي. ومع ذلك ، في مثل هذا النموذج الجديد للنظام ، فإن طلب خط دفاع محدد بوضوح من شأنه أن يتسبب في قلق المستخدمين المحتملين بشأن الكشف عن معلوماتهم الشخصية ، خاصة بالنسبة للمعارضين غير المصرح لهم أو الأشرار. تصف هذه الرسالة نظام مصادقة فعال وخفيف الوزن على طريقة ما بعد التشفير الكمي لحماية المعلومات الطبية للمريض في WBAN. تستخدم هذه الطريقة خوارزمية التشفير الغير متماثل لتشفير وفك تشفير البيانات السرية بطريقة ، وإنشاء المفتاح لتأسيس ذلك كان KYBER مع مخطط تشفير مستوى IND-CPA .

الكلمات المفتاحية : التشفير ما بعد الكمي ، بروتوكول المصادقة ، الأمن ، WBAN .

Table of Contents

List of Figures

List of Tables

General introduction

Nowadays, the Internet of Things (IoT) and it's widespread in the world and our daily life has brought new ways to facilitate and to help us improve every type of activity from waking up in the morning to managing daily routines in such way that nobody has ever thought before. Even to our medical condition that today there are multiple ways that a doctor can monitor a patient condition just by knowing their states by reading data collected by IoT applications and some sensors connected to a patient device, they are called Wireless Body Area Network, WBAN. It collects the data from the user and sends it to a certain station. In the other face it has brought us a huge challenge which is securing these data that no one can access more than the caregiver or patient or a trusted part. The security of data transmitted by the WBAN is very important because it contains sensitive data about the patient and needs to be in a high level of security, even though the WBAN doesn't have enough resources (energy or processing resources) to perform some well known security and ciphering techniques.

Statement of the problem:

- The search for ways to protect the security of WBAN is still understudy.
- Nowadays, the methods and techniques used by attackers to get information from WBAN are evolving because most personal information is at risk and threatened by theft.
- In addition, there is not a really authentication scheme that provides both lightweight and high security level.

Objectives:

- Our main objective is to propose a more lightweight secure authentication scheme for patient monitoring using WBAN in which communications are encrypted and secured by applying a secure encryption algorithm.
- Our authentication scheme should provide both lightweight and high security because we use it in devices that are low-powered and low computational resources.

Organization of the dissertation:

This manuscript is divided in four chapters:

In the first Chapter , We will discuss some important background information in IoT, healthcare and even WBAN, such as the use of IoT devices and application and it’s widespread , some concepts of WBAN and it is architecture and it’s medical applications .

In Chapter 2, we will discuss some concepts of security for the WBAN and Cryptography such as symmetric and asymmetric encryption, as well as the security requirements of WBAN.

In Chapter 3, we will introduce and quick analyze some related works.

In Chapter 4, we will try to show you our proposed scheme and explain how it works and what attacks it can prevent, explain how our chosen ciphering algorithm works and performance evaluation of it such as computational and communication cost.

Chapter 1

Background

Introduction:

In this chapter we will talk about what we had to search about and for to barely know what is going to face us during the process of producing a secure authentication scheme for WBAN and it is use in IoT medical field.

1.1. IoT and wireless body area networks :

Information technology and the Internet of Things (IoT) have become increasingly prevalent in many industries, including health care. The term "Internet of Things" (IoT) is more significant today than ever. The Internet of Things (IoT) outlines a situation in which not only personal computers and smart phones are linked, but common objects are turned into smart objects that can communicate and respond to their surroundings. Cisco predicts that the Internet of Things will have about 75 billion deployed units by 2025 . [1]

Demand for medical treatment and patient remote monitoring, or tele-health, has increased as the number of patients suffering from chronic and cardiovascular illnesses in advanced nations has increased, as has the overall aging of the population. Sensors attached to the patient's body, such as ECG electrodes, pulse oximeters, temperature, or blood pressure sensors, monitor the patient's physiological data regularly and broadcast it via the internet to devices accessible by doctors and caretakers. As a consequence, remote users can evaluate the patient's health and track his or her heart rate, temperature, blood pressure, and other vital signs.

The nature of patient information is quite delicate. As a result, there is a large issue in that this data is being transferred via the internet, which is a wireless public network vulnerable to intruder attack. Sensors are used in a hacker-prone environment, which allows attackers to intercept them and transmit erroneous data to caretakers, leading in a misdiagnosis [3]. They can also blackmail the sufferer by listening to the sensed data [3]. This compromises the patient's privacy and is especially difficult when the patient is observed in real time, since it means that all of his information will be available to adversarial attackers at all times.

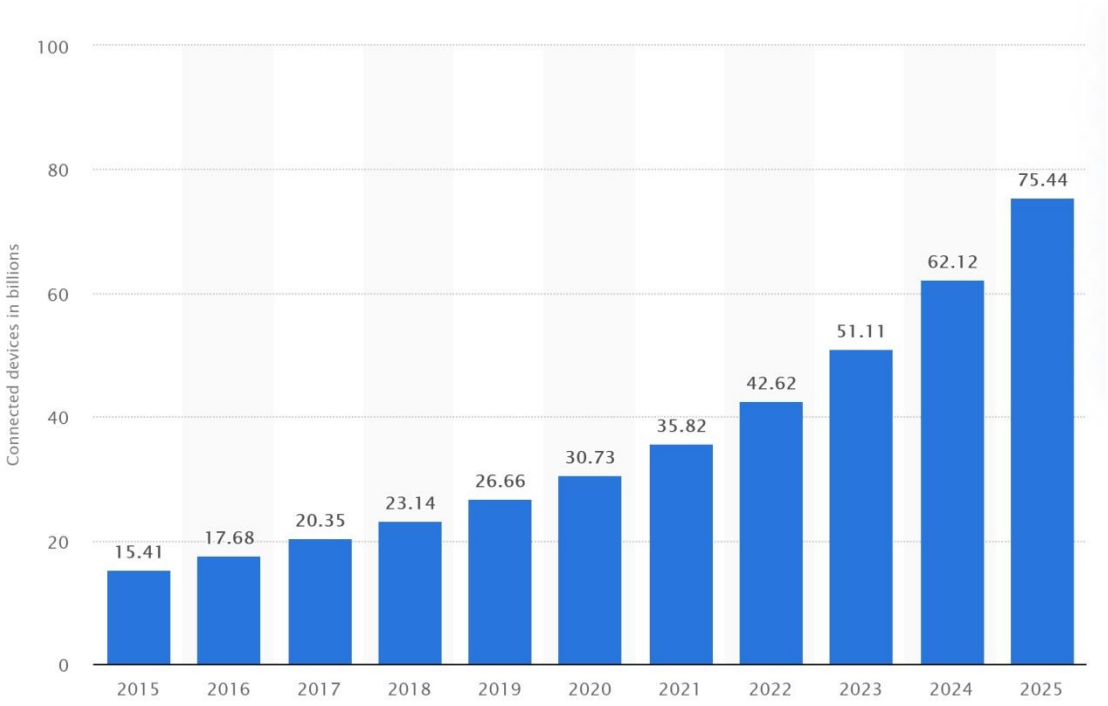

Figure 1.1 : Connected devices (billions) by year **[1]**

As a result, with a better user authentication method, significant care must be taken to prevent unauthorized access to the patient's confidential data. All remote users accessing the sensed data must be authenticated to avoid unwanted access. Also, the health professional should be able to verify the sensors from which they receive data and agree on a session key to encrypt communications sent back and forward between. This establishes a secure connection for key exchange between the remote user and the sensor nodes. Designing such protocols in BSNs with limited resources is especially difficult because we need to reach a compromise between security, privacy, and computational cost [1].

In today's world, wireless communication has a major application in sharing of information anywhere and at anytime. We can use wireless networks in the form of WLAN or WiFi in various fields such as education, healthcare, and industrial sector. As the technology is growing, the demands of users as well as the demand of ubiquitous networking is increasing. WBAN(Wireless Body Area Network) allows the user to move another without having the restriction of a cable for sharing information. The term 'Wireless Body Area Network' was coined in 2001 by Van Dam. It basically is a network containing sensor nodes that are attached to the human body, used to measure the bio

signals (heart rate, blood pressure, brain signals, etc.) of humans. It has majority of applications in medical sector.

A Wireless Body Area Network (WBAN) connects independent nodes (e.g. sensors and actuators) that are situated in the clothes, on the body or under the skin of a person. The network typically expands over the whole human body and the nodes are connected through a wireless communication channel. According to the implementation, these nodes are placed in a star or multihop topology [4].

A WBAN offers many promising new applications in the area of remote health monitoring, home/health care, medicine, multimedia, sports and many other, all of which make advantage of the unconstrained freedom of movement a WBAN offers. In the medical field, for example, a patient can be equipped with a wireless body area network consisting of sensors that constantly measure specific biological functions, such as temperature, blood pressure, heart rate, electrocardiogram (ECG), respiration, etc. The advantage is that the patient doesn't have to stay in bed, but can move freely across the room and even leave the hospital for a while. This improves the quality of life for the patient and reduces hospital costs. In addition, data collected over a longer period and in the natural environment of the patient, offers more useful information, allowing for a more accurate and sometimes even faster diagnosis.

1.2. **The WBAN Architecture:**

Each sensor in the WBAN design is seen as a node and each node is either placed on the human body in the form of the wearable device or implanted inside the human body. Each node is a sensor that collects and stores data.[4] In this network, collect human physiological vitals. transmit some info and interact with other nodes mobile devices that serve as gateways, There are three Tiers of wireless body area communication architecture depicts three nodes in a network similar to that established in.The architecture can support more than a hundred nodes. the form of the implanted device or the wearable gadget The body of a person In this network, each node represents a sensor that gathers and stores data. Collect human physiological vitals, transfer information, and communicate with other nodes. [10]

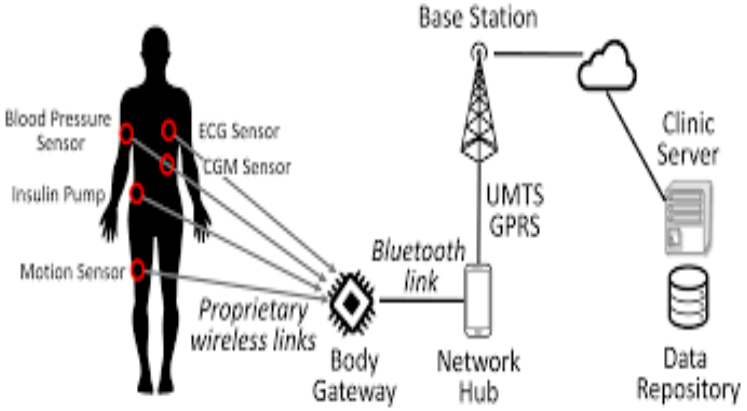

Figure 1.2: Architecture of WBAN [7]

1.3. **WBAN-Enabling Technologies**

WBAN is a breakthrough technique that was made possible by advancements in numerous technologies such as BLE, sensors, and network protocols. The following are technologies that allowed WBAN [13].

1.3.1. **Bluetooth Low Energy (BLE) technology:**

Bluetooth Low Energy is an extension of the Bluetooth protocol that is better ideal for WBAN since it uses less electricity [8] with the assistance of a low duty cycle. It was created to work wirelessly with small mobile devices that are too small to support the power consumption of standard Bluetooth technology. It has a data rate of 1 Mbps [13].

1.3.2. **ZigBee:**

ZigBee is one of the wireless technologies that works in a low-power consumption environment. Its targeted application radio frequency (RF) applications with low battery use, low data rate, and improved security are described by the ZigBee specification. ZigBee's security is ensured by its 128-bit secure authentication scheme, which ensures assured privacy and integrity. ZigBee-based devices may function for several years without changing batteries thanks to sleep mode [10].

1.3.3. **IEEE 802.15.6**

IEEE 802.15.6 is the first WBAN standard, and it applies to both medical and non-medical applications of WBAN. It also aids communication both outside and within the body. For data transmission, this standard employs a variety of frequency bands,

including narrowband, ultra-wideband, and human communication band. This is a critical step toward implementing WBAN because it encourages researchers to develop wearable sensors with low battery consumption, a wide frequency range, and a sufficient number of nodes per body and priority nodes based on application requirements [9].

1.4. **WBAN Medical applications**

We can use WBAN to monitor physiological parameters such as blood pressure, body temperature, and heartbeat.[12]. Now that the parameters that we collected have been sent to a remote server for processing, the appropriate action can be taken. WBAN can be used to detect and treat patients in the early stages of sickness, which might be highly advantageous for some major illnesses such as hypertension anddiabetes [13, 14].

WBAN Field of Application	Type of application	Wearable	Non-wearable	Implant	Application
Health care application	Medical	Yes	No	No	ECG
Health care application	Medical	Yes	No	No	Electromyography (EMG)
Health care application	Medical	No	No	Yes	Diabetes Control
Health care application	Non - Medical	Yes	No	No	Electromyography

Table 1.1: Applications of WBAN [10]

1.5. **WBAN Challenges**

Although WBAN technology has advanced significantly in recent years, various researchers have explored and reported on a number of issues linked to its real-time applications . The most significant WBAN difficulties are listed below.

Security and Privacy: As these systems deal with the exchange of patient's data, they require high level security and privacy. The design constraints of the network must be chosen in such a way that it does not combine the parameters of one patient with another by providing limited access to the data. The data transfer methods prescribed for WSN are not suitable for WBAN. Confidentiality, authentication, integrity, freshness of data along with availability and secure management contribute to the security requirements of WBAN and pose as one of the greatest challenges in providing secure WBAN system [15].

1.5.1. Data Authentication

In both medical and non-medical applications, data authentication is required. Both the WBAN nodes and the coordination node require confirmation that data is being sent from the trust center and not from a rogue node. By exchanging a secret key, they compute a Message Authentication Code (MAC) for all data. The network coordinator will recognize that the received message was transmitted by a trustworthy node after the right MAC has been determined.

1.5.2. **Interference:** During the large-scale implementation of WBAN , the wireless link established between the sensors uses radio signals that may interfere with other network devices. [10]

1.5.3. **Data management:** To keep the data collected continually for monitoring the health of patients for quick access and retrieval, a huge database is required. It is also necessary to take the necessary precautions to avoid data collisions Sensors used in WBAN systems must be power efficient and reconfigurable, with minimal complexity, small form factor, light weight, and simple operation. The storage device should be designed to allow flexible access to the patient's medical history at any time for external processing and analysis utilizing internet technologies.[12]

1.5.4. **Interoperability:** For information interchange and plug-and-play device engagement, WBAN systems must guarantee data transmission across protocols such as Bluetooth and Zigbee. Systems must be scalable in order to provide a steady connection and fast network migration. [26

1.6 Sensor Nodes

Single sensor nodes are commonly referred to as motes in the context of WSNs . They typically feature a CPU, wireless radio, and a variety of sensors. Motes collect environmental data and communicate it via radio connection to a central entity known as the data sink, or simply sink. They are also frequently fitted with large antennas to cover a greater distance and a battery slot for the energy supply. Figure 1 depicts an IRIS and a TelosB mote, both of which are equipped with the aforementioned.

Figure 1.3: IRIS and TelosB CM5000-SMA motes [10]

Motes come in a variety of flavors in practice. The physical dimensions and processing power required vary greatly depending on the application. The proportions of motes range from Weather stations, for example, to microscopically tiny particles in military applications, dubbed smart dust. As a result, the deployment of motes varies. Some motes may be dropped at random (for example, from an airplane) or put on purpose at a specified spot. Table 1.2 provides an overview of frequently used WSN motes and their technical specs to demonstrate the resource variation between different hardware platforms.

Mote	RAM [KB]	Flash [KB]	CPU [MHz]	Bus [bit]	Energy supply
TelosB	10	48	4-8	16	2x AA battery / external
MicaZ/Mica2	4	128	8	8	2x AA battery
IRIS	8	128	8	8	2x AA battery
OPAL	52	256	96	32	3x AAbattery / external
Rene	0.5	8	4	8	1x button cell

Table 1.2: List of popular mote platforms and their hardware specifications [10]

1.7 WSN Components

As many authors note, it is often beneficial to assign different roles to WSN motes, most often to provide aggregation of collected environmental data. The idea is to shift from an address driven routing, where data is sent on the shortest path to the end-node, to a data driven routing, where data streams are combined in a meaningful way on the path to the destination. Min et al. have shown that the overall energy requirement for independent transmission of individual measurements towards a central entity is a lot higher than for aggregation and transmission of a combined data set once over the longer distance. To visualize the idea, imagine a scenario where a user is interested in receiving measurements from all sensor nodes, but only to check if the average value has changed. For example the room temperature could be measured with several sensors in a single room, but the A/C control should only interfere if the average temperature has changed significantly. [5]

1.7.1 Nodes that collect data

Collectors are only allowed to gather and send environmental data. They do not perform any preprocessing on the data they gather; instead, they send simply raw data. Humidity, temperature, light, and voltage are just a few examples. Measurements are carried out on a regular basis, followed by data transfer to the sink.[17]

1.7.2 Nodes that act as Aggregators

The Aggregators in this thesis differ from others in that they do not gather sensor data on their own; instead, they are solely employed to process messages and signal the results. This isn't a typical need, but it was used in the thesis implementation since TelosB motes don't have the memory or computing power to do additional tasks like reading sensor data. The existing implementations allow you to adjust the degree of aggregation (doa), or the number of transmissions, during runtime.

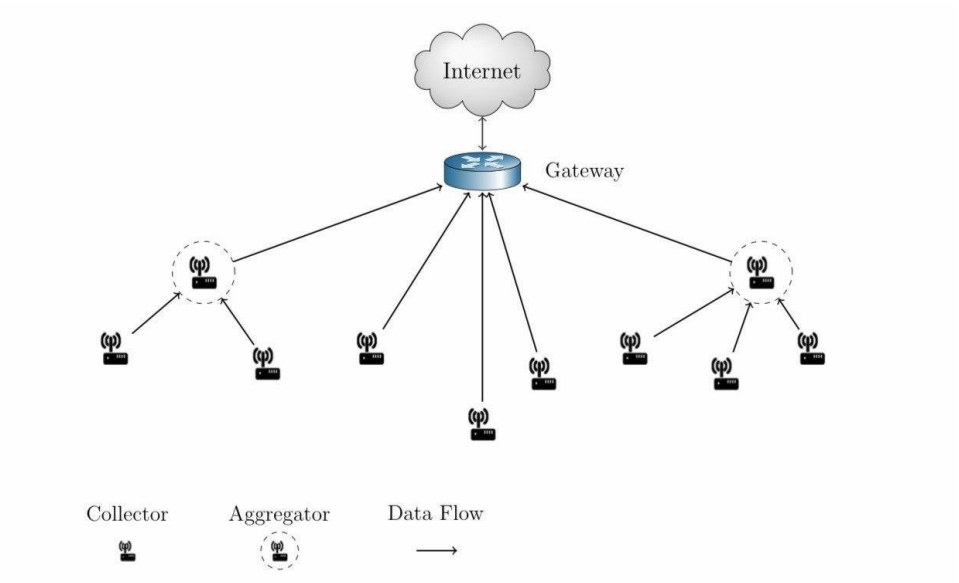

Figure 1.4: Typical WSN topology with Collectors and Aggregators.

1.7.3 Gateway

In a WSN, the Gateway plays a unique role. It establishes a connection between the local WSN and the Internet and routes data between the two networks. A bridge between the IEEE 802.15.4 wireless personal area network (WPAN), which is utilized in WSNs, and the Internet is usually included. This bridge is typically made up of a sensor node (also known as a base station) and a server that is linked to the Internet. Gateway is the name given to the resultant complex, which is seen in Figure 2. In most cases, the Gateway just forwards communications and does not preprocess data. Individual data forwarding procedures, such as header de-encapsulation, cannot, however, be ascribed to a single Gateway component. As a result, it is frequently treated as a single entity.

Chapter 2

Security of WBAN Systems

2.1. Cryptography :

To insure the security for our data that will be gathered by the wireless sensors or the WBAN and transported over the internet where everyone has access to , we need to perform some techniques and algorithms called cryptography algorithms and cryptography schemes that consists of a variety of techniques .

Human being from ages had two inherent needs (a) to communicate and share information and (b) to communicate selectively. These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand.

2.1.2. Cryptography algorithms :

There are a lot of cryptography algorithms, each one works with a different mechanism and options and that causes different vulnerabilities for each one either. Nowadays, encryption technology is mostly associated with scrambling plain text into encrypted text and it is followed by a return to plain text. Decryption is the term for this procedure. Therefore, encryption and decryption are accomplished using a variety of algorithms. The most prosperous Algorithms work with keys. The key is just a parameter in the algorithm that enables encryption and decryption procedure. The area of key-based cryptography algorithms nowadays may be classified into two categories. Symmetric-key cryptography and asymmetric cryptography are two types of cryptography. Cryptography using public keys. Symmetric-key encryption is a type of encryption in which the keys are symmetric. Both the sender and the recipient have the same encryption key. [5]

Encryption using a public key is known as public key encryption .To ensure that a communication arrives safely, it must be encrypted and decrypted .Another security measure The cryptographic hash function is a technique that employs mathematical transformations to solve problems . "Encrypt" information permanently.

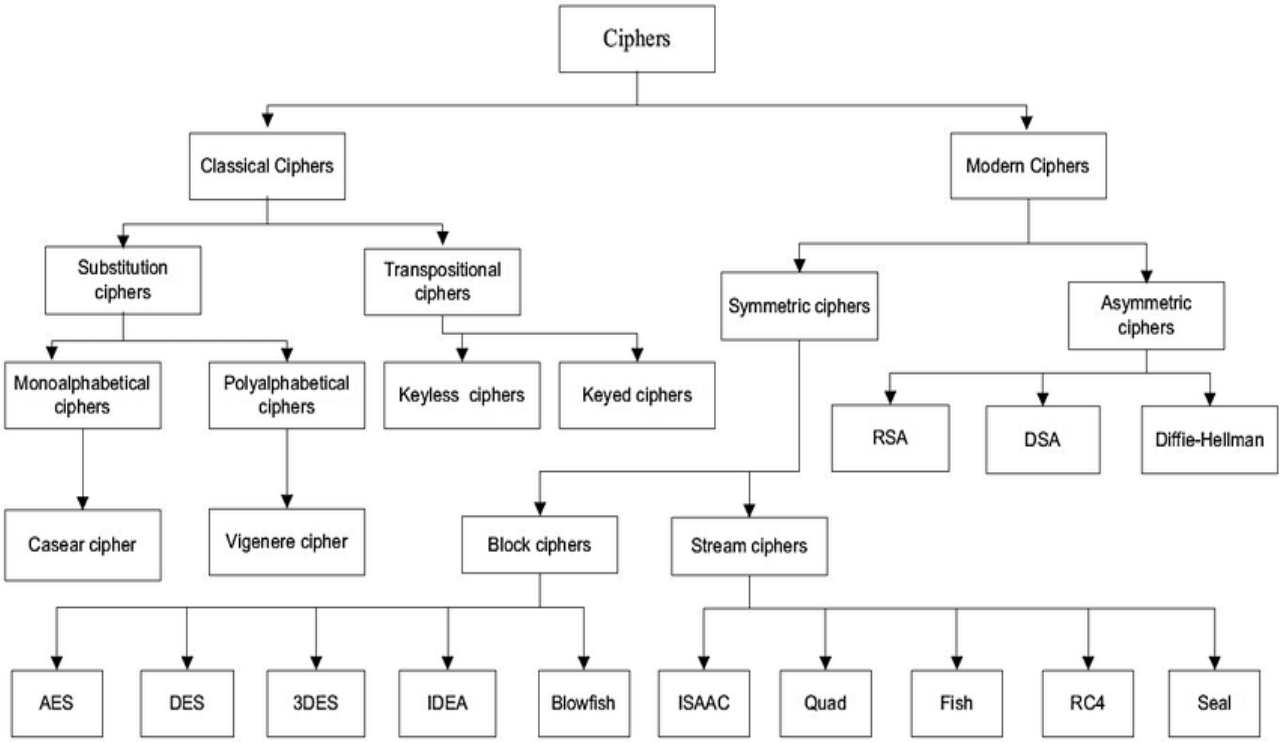

Figure Some of cryptography algorithms and techniques

2.1.3. Symmetric-Cryptography :

Symmetric cryptography systems are also known as symmetric-key, secret-key, and other terms and single-key algorithms or schemes The easiest way to introduce symmetric cryptography is to use it. [7]

Begin with an issue that is simple to comprehend. Alice and Bob, two users, are interested into connect via a public network that isn't secure. The name "channel" may appear to be a misnomer. It may sound a little esoteric, but it's only a name for the communication link: This could be the case. The Internet, a sliver of air in the case of mobile phones or wireless LAN transmission, or any other form of communication you may imagine. The real issue begins here. For example, consider the evil man Oscar1, who gained access to the channel by hacking either connecting into an Internet router or listening to radio signals of a Wi-Fi communication .[5]

Obviously, there are many situations in which Alice and Bob would prefer to communicate without Oscar listening. For instance, if Alice and Bob represent two offices of a car manufacturer, and they are transmitting documents containing the business strategy for the introduction of new car models in the next few years, these

documents should not get into the hands of their competitors, or of foreign intelligence agencies for that matter.

In this situation, symmetric cryptography offers a powerful solution: Alice encrypts her message x using a symmetric algorithm, yielding the ciphertext y. Bob receives the ciphertext and decrypts the message. Decryption is, thus, the inverse process of encryption. What is the advantage? If we have a strong encryption algorithm, the ciphertext will look like random bits to Oscar and will contain no information whatsoever that is useful to him.

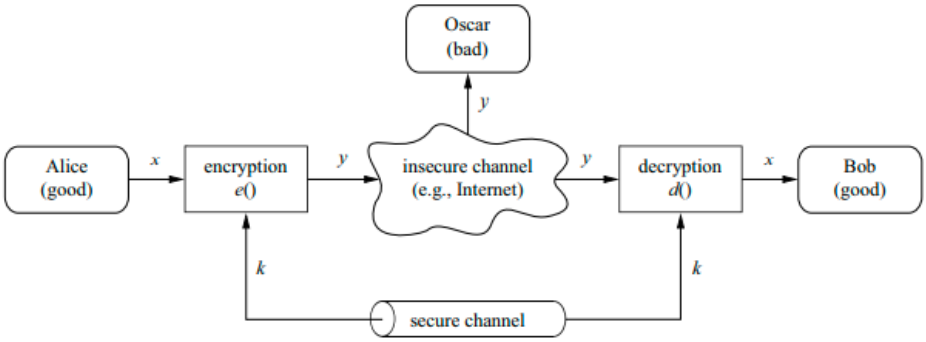

Figure 2.2: Symmetric cryptography , how does it work

2.1.4. Asymmetric cryptography

Also known as Public-key cryptography is a newer developed cryptography that encompasses creating secret keys that can decode encoded messages. Mentioned previously, the cryptography that has been with us throughout history is symmetrical, which means that it uses the same key for encryption and decryption, but that can pose issues if the key itself is not secure, thus others can interfere, and simply the number of keys needed. [5]

To ease this situation, asymmetrical cryptography was created that first prioritizes creating a safe key on one end, then the receiver has a matching key. We can show RSA encryption as a public-key encryption example. RSA algorithm is used for digital signatures and public encryption. It is a simple algorithm based on modular exponentiation of large integers.

This type of algorithm involves creating a public key that anyone can use to encrypt and a private key that can only be used between the parties. The private key is

transferred to the other party using a one-way algorithm. The message is protected because the corresponding private key is needed to decrypt the message.

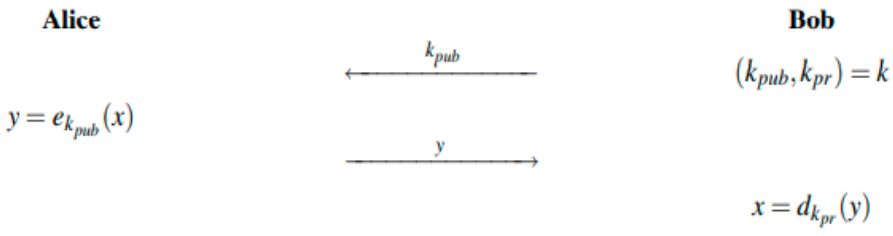

Figure 2.3: Asymmetric cryptography [5]

- **Hash functions :**

Hash functions are just simple functions, they accept a certain length of input and compress it into a shorter fixed-length output. Any changes to the original input data will cause the hash code to change. The value returned by a hash function is called a hash value, hash code, digest or hash.

- **One-way function** :

A function *f()* is a one-way function if:

1. $y = f(x)$ is computationally easy, and

2. $x = f^{-1}(y)$ is computationally infeasible.

2.2 Post-quantum cryptography :

Although a fully-functioning quantum computer does not exist yet, researchers are still looking into ways to advance that technology of a quantum computer and are coming up with safety measures for its debut into our daily lives.

Fundamentally, a quantum computer should be able to take multiple inputs at once and process them simultaneously while factoring in the other inputs, similar to how we process many different functions at once in our brains. This large amount of processing is done on a singular computer system. This makes quantum computing

vastly different from classical computing. In classic computing, computers are only able to use one decision at a time in a logical and series 13 method.

The future of quantum computers suggest that the development could lead to major improvement in many areas including health and safety for it's capability to be used with Artificial Intelligence. The basis of quantum computing comes from quantum theory. Quantum theory is still in development, but summarily, it consists of looking into a quantum world that contrasts the physical world and science we see everyday. In the quantum world, there are three distinct properties [7]

2.2.2 Quantum versus Post-Quantum Cryptography

With the increasing need for cybersecurity protections, two different solutions were found: quantum cryptography and post-quantum cryptography. In this portion, we will briefly discuss both of them and how each impacts quantum computing, then why post-quantum cryptography is more effective. Each statement is brief because there is still much research needed on both options as quantum computers are developed into a fully functioning machine.

Quantum cryptography uses a quantum channel in order to send quantum bits, the storage for communication, from one location to another. This process is ideal for short distances, but in long-distance communications, facilities such as quantum satellites and repeaters will be needed to allow for communication all over the world. On the other hand, post-quantum cryptography uses ciphers and matrix mathematics.

Matrix mathematics is believed to be protected from quantum attacks in comparison to classically used methods (e.g. discrete mathematics and factoring) which quantum computers are able to decipher. Matrix manipulation provides more dimensions that will make it difficult for a quantum attack to occur despite the multiple processes it uses Although both options are useful to have, post-quantum cryptography provides for less facilities built and is able to reach long distances easily, albeit computation assumptions are necessary to get it working; therefore, it was decided by the National Institute of Standards and Technology (NIST) that there needs to be a process to standardize post-quantum cryptography so when the devices come out, we are prepared to handle quantum attacks [18].

2.3 Attacks In Wireless Body Area Networks

2.3.1 Denial of Service (DoS) Attack:

The adversary may use digital communication to interface with or damage the WBAN, resulting in the transmission of extra data packets that the WBAN system may not be able to manage. As a result, authorized users may be barred from accessing the essential data. The WBAN system is severely disrupted as a result [19].

The physical layer: The physical layer is responsible for frequency selection and creation, signal detection, modulation, and encryption, among other things [25]. Because the medium is radio-based, it is always feasible to disrupt the network. Jamming and tampering are the most typical physical layer assaults.

2.3.2 Jamming attack

Jamming is a typical physical attack that attackers may easily carry out when the wireless transmission frequency utilized in a WBAN is known. In this type of assault, an attacker sends out a radio signal at a random frequency while the sensor nodes give out communication signals. The radio signal interferes with another signal provided by a sensor node, preventing the attacker from receiving any messages within range. As a result, nodes in the range of any attacker signals become completely isolated, and no messages may be sent or received between the impacted nodes and other sender nodes as long as the jamming signal is active [28].

2.3.3 Tampering attack

Sensor networks are typically used outside. The nodes in a WBAN are especially vulnerable to physical assaults due to their unattended and scattered nature. Physical strikes on nodes may result in reversible harm. The attacker can use the seized node's cryptographic keys to alter data, modify program codes, or even replace it with a malicious sensor. Sensor nodes, such as MICA2 motes, have been shown to be vulnerable in less than one minute [25].

2.3.4 Exhaustion of Resources

Because of resource depletion, denial of service (DoS) assaults occur. A native link layer implementation, for example, may attempt to transmit the damaged packets indefinitely. The energy reserves of the retransmitting node and those around it will swiftly decrease unless these futile retransmissions are discovered and halted [34].

2.3.5 **Network Layer Attacks**

WBAN nodes are not obligated to route packets to other nodes. When many WBANs interact with each other through their coordinators, routing is feasible. Spoofing, selective forwarding, sinkhole, wormhole, Sybil, and hello flood are all possible assaults.

2.3.6 **Selective Forwarding**

Selective forwarding is a type of attack in which a hacked or malicious node removes packets it likes and selectively forwards packets to make surrounding nodes suspicious. When these malicious nodes get closer to the base station, the harm becomes more powerful. Against a selective forwarding attack, there are two types of defenses that have been proposed. The first entails detecting compromised nodes and routing data to an alternate way, while the second entails transmitting data via multi-path routing

2.3.7 **Hello Flood Attack**

In a Hello Flood attack, the attacker delivers a hello message to the network along with a highly strong radio signal to persuade all nodes to route their communications through the attacker. Authentication is a good countermeasure to the Hello Flood assault. Authenticated broadcast protocols, are an effective technique. The sections below provide more information. A recent article presents a countermeasure to the Hello Flood attack that entails using a probabilistic secret sharing mechanism and bidirectional verification.

Network Layer	Attacks	Countermeasures
Physical Layer	Jamming	Detect and sleep, route around jammed areas
	Node tampering	Tamper-proof boxing
Link layer/ medium access control	Collision, unfairness	Authentication and anti- replay protection
	Daniel of sleep	Authentication and anti- replay, detect and sleep, broadcast attack protection
Network and routing layer	Neglect and greed, misdirection, spoofing, replaying, routing- control traffic or clustering	Authentication and anti- replay protection, secure cluster formation
	Homing	Header encryption and dummy packets
	Hello floods	Pair- wise authentication, geographic routing

Table 2.1: Attacks and Countermeasures at Each Network Layer [18]

2.4 Security Requirements in WBANs

Even though security issues are made a high priority in most networks, little study has been done in this area for WBANs. Additionally, because of strict resource constraints in terms of memory, power, computational capability rate, communication and as well as inherent security vulnerabilities, the security specifications proposed for other networks are not applicable to WBANs [18].

Practically, deployment of WBANs and the integration of convenient security mechanisms need knowledge of the security requirements of WBANs pointed out that the authentication scheme for remote patient monitoring should satisfy many security requirements, including strong user authentication, mutual authentication, confidentiality, session key establishment, low communication and computation cost, data freshness, and secure against different kinds of popular attacks, such as impersonation attack, replay attack, and password guessing attack. Due to the sensitivity of physiological data, we believe that an authentication scheme for remote patient monitoring should also meet the following security properties. Forward Secrecy. [19]

The authentication scheme provides forward secrecy, which means that if an adversary acquires the long-term keys of the user, the gateway, and the wearable sensor node, he/she cannot access the session keys generated in previous sessions. Conversely, if authentication scheme fails to provide forward secrecy, it may cause the disclosure of the session keys used in previous communications and the disclosure of the patient's sensitive information. To ensure the secure transmission of sensitive information, authentication [20].

2.4.1 Data Integrity

When data is transmitted to an insecure WBAN, sometimes, its information can be altered. An adversary will then be able of adapting a patient's information prior to reaching the network coordinator, so endangering the patient's health and maybe even their life. As a result, the received data requires to be assured of not being altered by an adversary through right and correct data integrity by using data authentication protocols. [16]

2.4.2 Data Confidentiality

Protection of data from disclosure can happens through data confidentiality. The role of WBAN nodes in medical applications is transmitting sensitive information concerning the status of a patient's health. Critical information can be eavesdropped, which may cause a considerable amount of damage towards a patient as the data issued for illegal goals. Data confidentiality can be accessed through encryption of a patient's data via a shared key on a communication channel secured among the WBAN nodes and their coordinator [14].

2.4.3 Data Freshness

Data integrity and confidentiality can only be supported if data freshness techniques are used. An adversary has ability to capture data in transmissions and then replay it to create confusion for the WBAN coordinator. Data freshness assures that data is not reused and its frames are in order. There are two different types of data freshness as follows: strong freshness that guarantees delay as well as frame ordering, and weak freshness which provides no guarantee in terms of delay. Strong freshness is essential in synchronization while a beacon is being transmitted to WBAN coordinator, whereas weak freshness is important for WBAN nodes with low duty- cycle. [14]

2.4.4 **Availability** The availability of the patient's information to the physician needs to be ensured at all times. An attack towards availability in WBANs could be capturing and disabling an ECG node leading to loss of life. Therefore, maintenance and capability to switch to another WBAN in case of availability loss is vital. [20]

2.4.5 Data Authentication

Data authentication is a necessity in both medical and non-medical applications. Both WBAN nodes and the coordinator node need verification that data is being sent from the trust center and not a false adversary. Both of them compute a Message Authentication Code (MAC) for all data by sharing a secret key. When the correct MAC is calculated, the network coordinator will realize that the received message is being sent by a trusted node. [20]

2.3.6 Forward Secrecy:

The authentication scheme provides forward secrecy, which means that if an adversary acquires the long-term keys of the user, and the wearable sensor node, he/she cannot access the session keys generated in previous sessions. Conversely, if authentication scheme fails to provide forward secrecy, it may cause the disclosure of the session keys used in previous communications and the disclosure of the patient's sensitive information. To ensure the secure transmission of sensitive information. [19]

2.4 Authentication schemes :

An authentication scheme is a module that implements a way for a user to authenticate itself to the stations that he is communicating with . In particular, an authentication scheme checks credentials presented by the user against some data store containing user information, and determines whether the credentials match those stored in the data store.

There are several attacks that break authentication , and from this we tried to see some predefined authentication schemes and their weaknesses against some types of attacks that our proposed scheme prevents .

2.5 Lightweight security :

As its name implies, lightweight security deals with the same security concerns as its conventional counterpart, however in a reduced, i.e. "lightweight", capacity. It too covers a wide range of topics including both cryptographic algorithms and protocols. Despite being a relatively new topic, it has been attracting researchers, thanks to the rapid deployment of IoT. The main question in field is to achieve "sufficient" level of security given the limited capability of the target platform, which in fact is a challenging target.

Conventionally, security within an algorithm is ensured by the complexity of the underlying security algorithms and hence the corresponding operations. These operations do not only require heavy processing, but are also memory and storage consuming. Clearly, it is a practical impossibility to provide any of these on an IoT platform. Implementation of these algorithms have to be optimized for certain platforms.

CHAPTER 3

Related works

3.1. Introduction:

In our process of forging a new lightweight authentication scheme for WBAN we had to discuss some points in which we are going to specify our main goals that we should attempt during this process.

We had to go a little back and see what we need to provide as security requirements for such domain, and see the previous works of certain researchers, analyze and discuss their issues and what they missed. We will bravely talk about security requirements and then we will see some related works to our project.

3.2. Related works:

Authentication is an essential security measure for the authorized user to access the patient's sensitive information collected by wearable sensor nodes. Until now, lots of lightweight and efective authentication schemes had been proposed for healthcare applications.

- **E-SAP :** In 2012, an efcient and lightweight authentication scheme, named E-SAP, was proposed by Kumar et al. for healthcare applications using wireless medical sensor networks (WMSNs). Tey claimed that the scheme was secure and resisted multiple types of attacks. [14]

- **He et al.**: in 2013 , He et al indicated that the scheme E-SAP failed to provide user anonymity. Moreover, their scheme was vulnerable to the privileged-insider attack and the of-line password guessing attack. To conquer the mentioned weaknesses, they presented a robust and efcient authentication scheme for healthcare applications using WMSNs. However, a series of articles pointed out that the scheme in He et al. still had some drawbacks and faws, such as user impersonation attack, of-line password guessing attack, forward secrecy attack, and lack of wrong password detection mechanism. [12]

- **Srinivas et al :** in 2017 Srinivas et al pointed out that the scheme He et al of insider attack and user impersonation attack. To handle these drawbacks, an authentication scheme using only computationally efficient operations was proposed for WMSNs.[20]

- **Das et al :** in 2017 Das et al indicated that user anonymity was not provided in the previous scheme. In addition, the scheme could not withstand sensor node capture attack and privileged-insider attack . To overcome the security weaknesses, they presented an

efcient and secure authentication scheme for WMSNs and claimed that the enhanced scheme was secure against possible known attacks and ofered additional functionality features. [20]

- **Wu et al** : In 2017, Wu et al. deemed that Das et al scheme had weaknesses Security and Communication Networks such as of-line password guessing attacks, and they were impractical if running. To overcome the historical security problems, a novel and lightweight two-factor authentication scheme for WMSNs was proposed, which provided user untraceability and met the desired security requirements. To ensure secure and authorized communication. [15]

- **Amin et al**. In 2018, presented an architecture for patient monitoring, and an anonymity and robust mutual authentication scheme was proposed. Tey claimed that their scheme was more robust and cost-effective than the existing schemes. [30]

- **Ali et al.** : In 2018 showed that the scheme in Amin et al was vulnerable to user impersonation attack, ofline password guessing attack, and known session key temporary information attack. In addition, they proposed an enhanced three-factor authentication scheme for healthcare monitoring. [5]

- **Chandrakar** : In 2019, Chandrakar presented a lightweight and robust two-factor authentication protocol for healthcare monitoring. Their scheme was efficient because only the hash function and bit XOR operations were used. Similar to some previous schemes, their scheme could not provide user anonymity and forward secrecy. Many authentication schemes based on asymmetric cryptographic techniques were also proposed for patient monitoring in the past few years discussed the overall system architecture and associated security requirements of a typical ambient assisted living system, and an efficient authentication protocol based on ECC was proposed subsequently.[28]

- **Hayajneh et al.** : In 2016 presented a lightweight authentication scheme based on public key technology, and the Rabin cryptosystem was implemented with diferent hardware settings using a Tmote sky mote to prove its efficiency. [20]

- **Challa et al**. In 2017 showed that the scheme of Hayajneh et al**.** was suspected to some desirable attributes, such as inappropriate mutual authentication and lacking of user anonymity. Besides, their scheme was vulnerable to many known attacks like stolen

smart card attack, of-line password guessing attack, privilegedinsider attack, and user impersonation attack. To counter these limitations and improve efciency, they presented a three-factor authentication and key agreement scheme with provably secure for healthcare, in which the lightweight ECC point multiplications was used . [20]

3.3. Discussion:

From the above analysis, we can see that though researchers proposed many lightweight authentication schemes for patient monitoring in the past, however, none of them provides both lightweight functionality and high security. The authentication schemes only using lightweight cryptographic primitives, such as the schemes in above failed to provide forward secrecy and sufered from the desynchronization attack. This motivates us to design a lightweight authentication scheme for patient monitoring, which provides more security and functionality attributes using post-quantum cryptography , specifically CRYSTLALS KYBER with ind cpa encryption / decryption for guaranteeing both lightweight security and high efficiency when it comes to cryptography .

Chapter 4
Proposed scheme and evaluation

4.1. Introduction:

As previously mentioned, the open nature of wireless medical sensor networks in a public untrusted environment makes them vulnerable to various security threats and puts the security and privacy of patient information at risk. This chapter introduces a lightweight KYBER-Based end-to-end, mutual authentication and key agreement protocol to be used in real-time wireless medical sensor networks between a patient or a doctor known as “USER” and a Trusted Server. Our scheme mutually authenticate the caregiver and trusted server. We claim that our scheme is lightweight despite its use of functions that has low computational and resource needs, and because deployment will be on the larger more resourceful medical devices connected to the sensors rather than the constrained sensors themselves.

Our scheme also uses dynamic identity to provide user anonymity and mitigate against user traceability. After successful key agreement, data from the sensor is encrypted before being sent directly to the caregiver, and only the trusted server can decrypt the messages so it’s an end-to-end encryption as well, we used a hash function, a biometric secure function and a post quantum public key encryption algorithm that is the kyber-512.

4.2. Main idea:

In this chapter, we propose a lightweight biometric based authentication and key agreement protocol to be used in body sensor networks that utilizes a Post-quantum cryptography called CRYSTALS-KYBER and dynamic pseudo-identity. To securely authenticate using biometrics, we use the cryptographic technique called fuzzy extraction which consists of two randomized operations. The generator function takes in a biometric credential and produces a secret string and a public accessory whereas the reproduction function takes in a noisy biometric credential and the public accessory to produce the right secret string if and only if the level of noise in the biometric template is less than a set threshold [11].

4.1.1. Mutual authentication :

Providing a complete scheme that can be deployed in a real-time environment across the doctor/nurse or patient and trusted server that insures authentication for both sides.

4.1.2. Caregiver and patient anonymity and prevention against traceability:

Our scheme protects both caregiver and patient identities. Also, dynamic identities are introduced to provide anonymity and untraceability of mutual authentication as these identities cannot be retrieved by adversaries without knowing secret random numbers. They are also updated in each round of authentication**.**

4.1.3. Lightweight authentication:

Our scheme is lightweight enough to be suitable for deployment on medical devices and body sensors or patient devices.

4.1.4. Biometric privacy protection

Through the use of fuzzy extraction: The generator function takes in a biometric credential and produces a secret string and a public accessory. The reproduction function takes in a noisy biometric credential and the public accessory to produce the right secret string if and only if the level of noise in the biometric template is less than a set threshold

4.1.5. Efficiency: We compare the performance of our scheme relative to others and show that our protocol has better performance.

4.3. Proposed scheme:

Our scheme consists of three essential phases, initialization phase, registration phase, login and authentication phase. The notations used throughout our scheme are presented in table 4.1 below. Please note that the remaining sections of this chapter we use "User" To describe the patient device that is already connected to sensors and uses it is own Interface to establish connections to a trusted medical server, it is a "User – Server" connection. We also use a post-quantum cryptography, called CRYSTALS-KYBER we will explain to you later.

Table 4.1: Notations and Abbreviations

Notation	Description
U_i	*User*
S	*Server*
SID	*Server Unique Identity*
ID_i	*Unique Identity of the user*
PW_i	*Password for login of user*
Bio_i	*Biometric imprint of user*
MID_i	*User Random Pseudo identity*
$Gen\ (\bullet)$	*Fuzzy Extractor parameter generation function*
$Rep(\ )$	*Reverse Fuzzy Extractor function*
Pk_S	*Public key of the server*
Sk_S	*Secret Key of the server*
Pk_U	*Public key of the user*
Sk_U	*Secret key of the user*
C_i	*Cipher text encrypted with kyber cpa enc*
$H(\bullet)$	*One way hash function*
$\|\|$	*Concatenate operation*
$\oplus$	*XOR operation*
$SKey$	*Session Key*

4.3.1. KYBER CPA Public Key Encryption :

Already in the early 2000s, cryptographers were becoming increasingly concerned about quantum computer breakthroughs. We know that a large enough quantum computer will break all widely used public key systems because of Peter Shor's famed Shor's Algorithm. RSA, finite field, and elliptic curve constructions are examples of this.

As a result, the National Institute of Standards and Technology (NIST) asked for new public key methods capable of withstanding quantum computers in 2017. One such planned post-quantum technique is Kyber. NIST judged it was worthy of standardization in 2021.

KYBER CPA PKE is a public key encryption mechanism that prevent from quantum attacks and it’s selected to be one of the most significant post-quantum cryptography algorithms, whose security is based on the hardness of solving the learning-with-errors (LWE) problem over module lattices.

4.3.1.1. **KYBER KEYGEN( )** :

This is the function that produces two values a public key and a private key .

The private key of a Kyber key pair consists of polynomials with small coefficients **S** .

A Kyber public key consists of two elements. A matrix of random polynomials A and a vector of polynomials t . Generation of the matrix is fairly simple, we just generate random coefficients and take them modulo q . .[17]

To calculate t we need an additional error vector e . This error vector also consists of polynomials with small coefficients, exactly like the private key Now we calculate **t** by matrix multiplication and addition : t = A*S + e

Private key = S

Public Key (A , t)

4.3.1.2. **KYBER Encryption ( )**

As in every public key encryption system, we can encrypt a message using the public key. Decryption can only be done by parties in possession of the private key.

The encryption procedure uses an error and a randomizer polynomial vector e1 and r . These polynomial vectors are freshly generated for every

encryption. Additionally, we need an error polynomial e2. The polynomials within e1, e2 and r are completely random, just like the ones in **S** .

Now, to encrypt a message **m**, we have to turn it into a polynomial. We do so by using the message's binary representation . Every bit of the message is used as a coefficient.

We encrypt m using the public key (A, t). The encryption procedure calculates two values (u, v) . A polynomial vector u and the polynomial v . [17].

4.3.1.3. KYBER Decryption ( )

To decrypt a given cipher text (u , v) we need to have a secret key sk .

4.3.2. Fuzzy extractor :

To securely authenticate using biometrics, a cryptographic technique called fuzzy extraction can be used. Fuzzy extraction consists of two randomized operations. The generator function takes in a biometric credential and produces a secret string and a public accessory. The reproduction function takes in a noisy biometric credential and the public accessory to produce the right secret string if and only if the level of noise in the biometric template is less than a set threshold.

4.4. Proposed protocol :

4.4.1. Initialization Phase :

In the first place we should initialize our system for it is future use and the first thing to to is to define system parameters for Kyber.cpa .

After that , the user device and the trusted server uses the key generation function to generate key pairs for each one , the user device generates a random integer and uses it as a UID, stores it's public key U_{PK} ,secret key U_{sk} , UID .

In the trusted server side , after key generation , Trusted server also generates a random integer and uses it as a server identification SID and stores S_{pk} , S_{sk} , SID .

4.4.2. Registration Phase :

In a secure environment public key exchange between user and trusted server should be already done , and both user device and trusted server have stored each one's Kyber-CPA public key .

(1) User U_i inputs it's ID_i as it's unique identity, a password PW_i, and imprints his/her biometrics Bio_i to the sensor of it's essential device . After that, the User device generates the secret biometric key R_i and public parameter P_i using the fuzzy extractor probalistic generation function $Gen(Bio_i) = (R_i , P_i)$.

After that, User's device computes Kyber-enc (PW_i , Pk_S) and computes a ciphertext C_1 ;

After that User's device computes A_i which equals $A_i = H(PW_i \,||\, R_i \,||\, C_1)$.

Then computes C_2 which is a ciphertext kyber-enc (ID_i , Pk_s) and then it get's the current timestamp T_1 , sends { C_2 , A_i } to the trusted server .

(2) Server gets the current time T_2 and checks weather $T_2 - T_1$ is below a defined threshold if true he continue the registration phase if not terminates the session .

Server computes UID_i by decrypting the ciphertext C_2 which will be done by kyber-dec (C_2 ,Sk_s) .

Checks weather UID_i already exists if not it generates a random value and sets MID_i = Random( ) and computes another secret value $B_i = H (ID_i \,||\, A_i \,||\, MID_i)$

And then it stores ID_i for future registrations , MID_i A pseudo Identity which will be used in the login and authentication phase , B_i which also will be used in the next phase .

After that it sends MID_i , B_i to the User's device that will store it and store P_i and C_1 .

USER SERVER

User inputs ID_i , PW_i , Bio_i ;

Gen(Bio_i) = { R_i , P_i } ;

C_1 ←Kyber.CPA.enc (PW_i , Pk_s) ;

A_i = H (PW_i || R_i || C_1) ;

C_2 ← Kyber.CPA.enc (ID_i , Pk_i) ;

Get the current timestamp T_1 and

sends data to the trusted server

{ C_2 , A_i , T_1 } →

Check Timestamp T_2 , computes T2 – T1

ID_i ← Kyber.CPA.dec (C_2 , Sk_s) ;

Check weather ID_i exists if not

Generate Random and sets MID_i = rand ()

B_i =H(ID_i || A_i || MID_i)

Store B_i , ID_i , MID_i

Sends Login data to USER's device

← {MID_i , B_i , SID}

Store: MID_i , B_i , P_i , SID in memory

Figure 4.1: The registration phase of the proposed protocol

4.4.3. Login and Authentication phase :

When it comes to login and authentication phase it's going to be in in-secure channel over internet so we should be preventing our data.

- The User inputs his ID_i* , Password PW_i* , his Biometric imprint Bio*
- And then the device extracts the pseudo-identity MID_i , the public parameter of the stored biometric imprint P_i , and a secret value occurred from encrypting the registration password C_1 .
- Computes Rep* (Bio_i* , P_i) = R_i* that is the secret value for the noisy parameter P_i .
- If R_i equals Gen(Bio_i*) then it's the real imprint of the real user so here we assume that the user is legit then computes $A_i = H (Pw_i || R_i* || C_1)$
- After that it computes timestamp value T_3 , Encrypts (MID $\oplus$ T_3) with the public key of the server Pk_s into a ciphertext C_3 , and kyber.cpa.enc ($A_i \oplus T_3$,Pk_s) into a ciphertext C_4 and sends a login request with the data { C_3 , C_4 , T_3 } .
- After the recipient of the login request from the user , the server get the timestamp value T_4 and check weather it's a real time request if true then decrypts the ciphertexts Kyber.cpa.dec(C_3 , Sk_s) into MIDi $\oplus$ T_3 and Kyber.cpa.dec(C_4 , Sk_s) into $A_i \oplus T_3$, compute $T_3 \oplus (MID_i \oplus T_3)$To get MID_i and $T_3 \oplus (A_i \oplus T_3)$ To get A_i .
- Then the server Extracts ID_i compute $B_i* = H (ID_i || A_i || MID_i)$ and compares it with the previous stored secret Value B_i , if B_i doesn't equal B_i* the server terminate session if it equals then it generates a new Random value MID_i* and Computes a new secret Value B_i* with MID_i* , $B_i* = H(ID_i* || A_i || MID_i*)$.
- After that the server and the user are authenticated and now computes a secret shared key for future communications , the shared key consists of a hash function for secret values computed in the previous steps , key = H (B_i* ||A_i || ID_i). Then the server stores MID_i* , B_i*. Get the current Time T_4.
- It calculates Kyber.cpa enc (MID*,Pk_u) into a ciphertext C_5 , compute $C_5 \oplus T_4$ into a value D_i and sends it to the user with the current time value .

- After the recipient of the message from the server that contains just a secret Value D_i , Checks the timestamp if it's legit then it computes the new random MID_i* generated by the server by $T_4 \oplus (C_5 \oplus T_4)$
- Gets a ciphertext C_5 that will need to be decrypted with Kyber.cpa.dec (C_5 , Sk_u) and gets the new pseudo Identity MID_i*.
- Then it computes the shared key by computing $B_i^* = H (ID_i \| A_i \| MID_i^*)$ $E_i^* = (B_i^* \| SID \| ID_i), SKey = E_i \oplus H (B_i^* \| ID_i \| A_i \| E_i).$

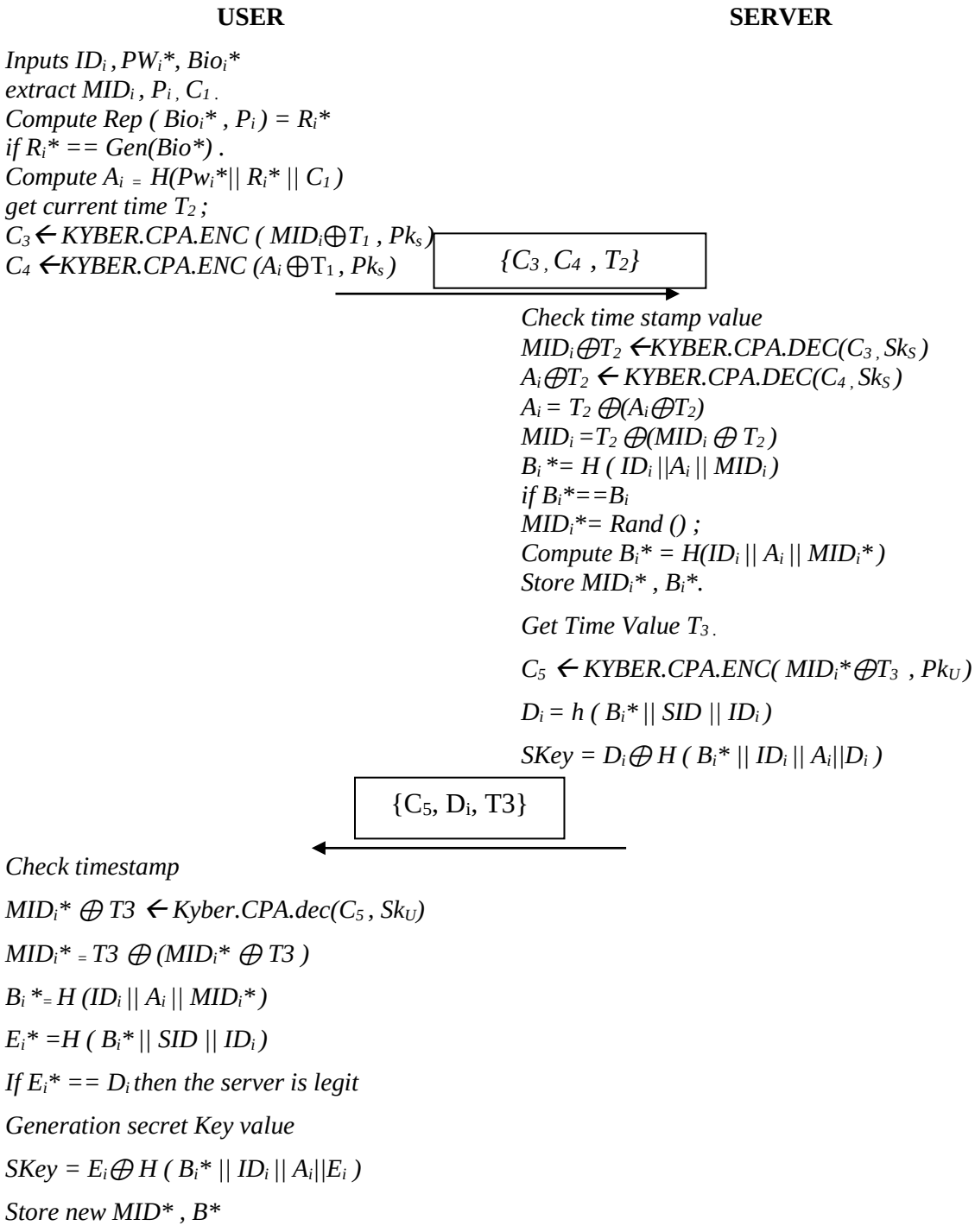

Figure 4.2: Login and Authentication phase of the proposed protocol

4.5. Informal Security analysis:

4.5.1. Mutual Authentication :

In the proposed scheme, the user and the server authenticate by checking A_i , B_i respectively which insure the legitimacy of the user and insure the authenticationof the server , and the server authenticate with the user by checking E_i and D_i .

4.5.2. Anonymity :

The proposed scheme we used a pseudo random identity MID_i which changes in every Login and authentication, and we insure it is security because it's crypted Two times so the listener will never get a chance to know it, or to know the previous one.

4.5.3. Session key establishment :

the session key is computed in the end of authentication protocol is used to encrypt the secret information during the communication and sending messages between the User and the server , the session key is symmetric both sides and one time used because it changes each session of communication . in our protocol User and Server calculate the session key $SKey = E_i \oplus H (B_i^* || ID_i || A_i || E_i)$.

4.5.4. Quantum attacks :

In the previous schemes no one insures security against quantum attacks, because they use encryption algorithms such as ECC, we used cryptographic algorithm based on ring-LWE IND-CPA Kyber which is powerful against all types of algebraic and quantum attacks

4.5.5. Biometric security :

In our scheme, we used a function called fuzzy extractor function which generates two parameters P_i and R_i, To insure the security of biometric data, at the same time this data can be used for verification and authentication

4.5.6. Forward secrecy :

Forward secrecy means that the encrypted communications and session keys in the past cannot be retrieved and decrypted even if the long-term secret keys are compromised. In the proposed scheme, if the long-term keys are compromised by an attacker, the confidentiality of past communications are not affected. Te reason is that the long-term keys are updated successfully by one-way hash function afer each session. Also Session key is established each time of authentication, and it depends on a dynamic values such as MID_i , and B_i .

4.5.7. Resist User Impersonation Attack :

In the proposed scheme, without knowing the password PW_i, the fingerprint information Bio_i, and the secret key Sk_U, the adversary is infeasible to forge a legal user and generate a valid message $\{C_3, C_4, T_2\}$. Therefore, the proposed scheme is resilient to user impersonation attack.

4.5.8. Quick Detection for Unauthorized Login

Quick detection mechanism for unauthorized login is essential for the authentication scheme. In the phase of user login, User device insure user legitimacy by computing the Value R_i* which is based on the noisy parameter P_i **,** and compares it with the input biometric imprint of the login *if* R_i* == *Gen(Bio*){* R_i*}* , so it can't perform and send a message to the server without the real value ; even thought the server computes a new value B_i and compares it with the previous one that depends on a real user informations , so the login won't be achieved until real values are applied.

Scheme	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9	I_{10}
F. Wu et al [8]	**Y**	**Y**	**Y**	**Y**	**N**	**Y**	**N**	**N**	**N**	**Y**
R. Amin et al [30]	**Y**	**Y**	**Y**	**N**	**N**	**N**	**N**	**N**	**N**	**N**
R. Ali, et al [15]	**Y**	**Y**	**Y**	**Y**	**N**	**Y**	**N**	**N**	**N**	**Y**
S. Challa et al [20]	**Y**	**N**	**N**	**Y**	**Y**	**Y**	**N**	**Y**	**N**	**Y**
X. Li. et al [22]	**Y**	**N**	**N**	**Y**	**N**	**Y**	**N**	**N**	**N**	**Y**
Our scheme	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**

I_1 Mutual authentication ; I_2 : User anonymity ; I_3Untraceability I_4 : Session key security ; I_5 Forward secrecy ; I_6 User impersonation attack ; I_7 Biometric security ;
I_8 : Desynchronization Attack ; I_9 Quantum attacks ; I_{10} : quick detection of unauthorized login

Table 4.2: Security Comparison between our protocol and some predefined schemes

4.6. Performance of our authentication scheme

We evaluate the computational and communication cost of the proposed protocol and compare it with the studied protocols.

4.6.1. Computational Performance :

This section will compare the computational efficiency of the proposed scheme with six state-of-the-art schemes. We focus only on the login and authentication phase of the proposed scheme, and the costs involved in registration and password change phases are not discussed because these phases are not used frequently. For the convenience of analysis, we define four computational notations T_h, T_{kenc}, T_{kdec}, and T_{fu} as the time cost of one-way hash function operation (using SHA-1 hashing algorithm), the Kyber encryption, Kyber decryption algorithms and a fuzzy extractor, respectively. Te bit XOR and concatenate operation is ignored here because it requires very low computation.

We evaluated the execution time of Kyber keygen , encryption , decryption , AES encryption , decryption , SHA512 on Kali Linux , Intel Intel(R) Celeron(R) CPU 1000M @ 1.80GHz with 3.89 GB of RAM , for the fuzzy extractor we did not found working implementations so we're going to take the execution time from a thesis .

We had to modify the implementation file in the speed test file test_speed.c because it was calculating speed by counting CPU cycles, so we included the time library time.h and we changed the counting from counting cycles to calculating (clock end – clock begin) / clock per seconds, and then we performed the command make speed to build and make the speed execution file and we got the results.

For SHA256 and AES, we made a text as input, we included the OpenSSL library and we made a C code for counting the execution time and here are results:

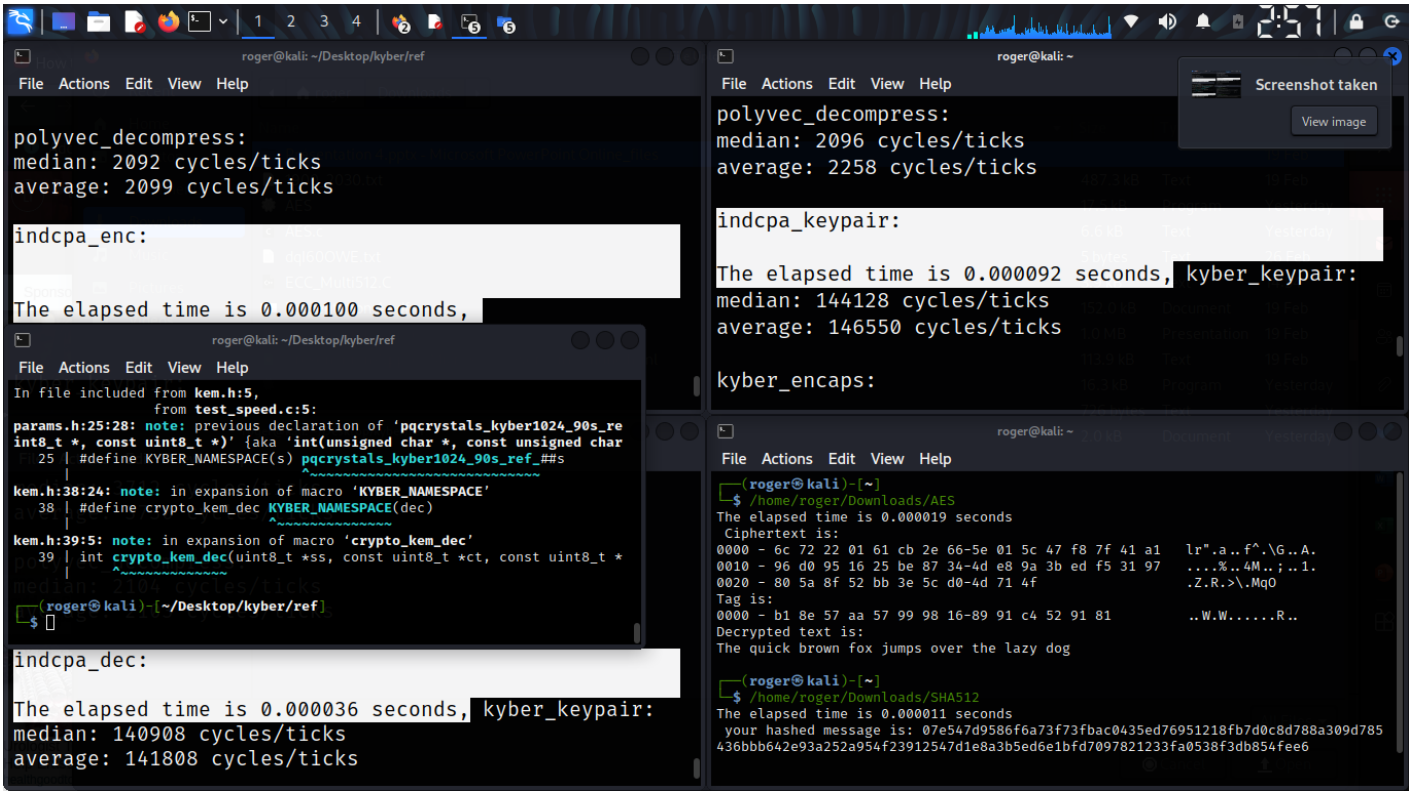

Figure 4.3: Calculation and evaluation of the execution time of every used cryptography algorithms

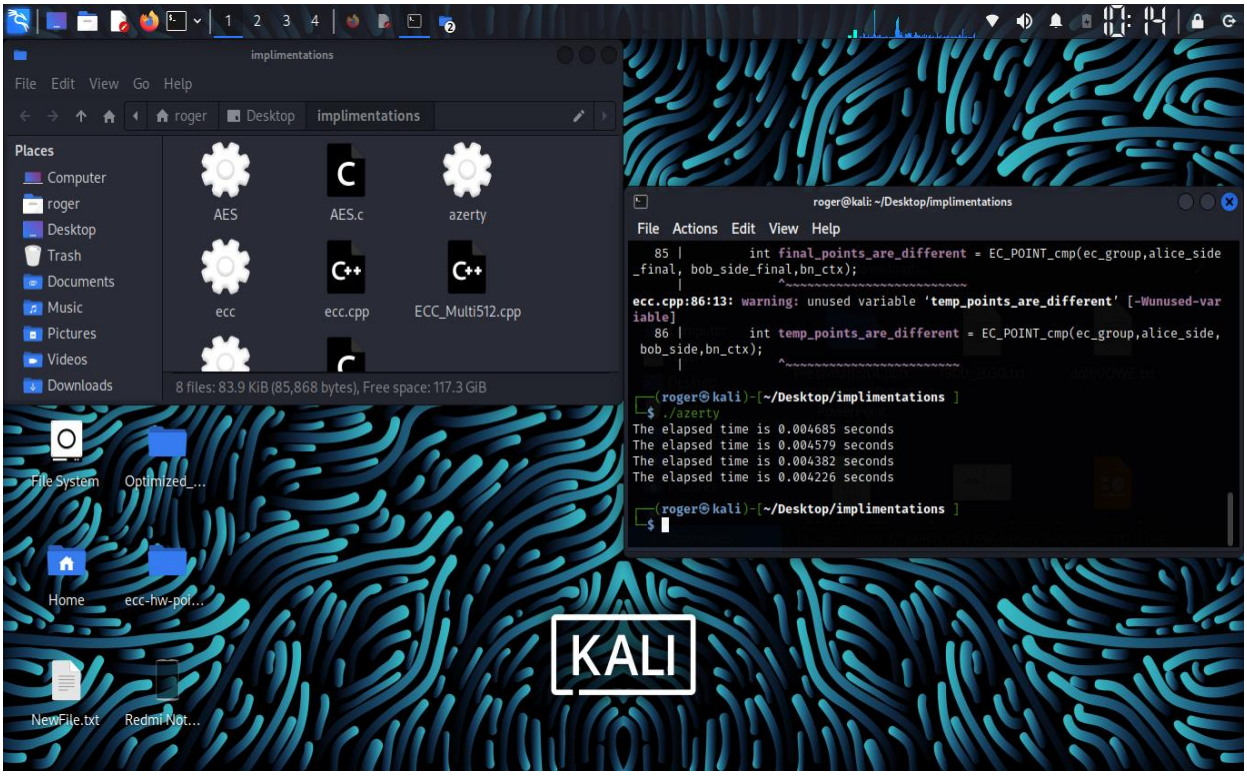

Figure 4.4: Execution time of ECC multiplication

Notation	Execution time
T_{keygen}	0.000092 second ≈ .092 ms
T_{Kenc}	0.0001 second ≈ 0.1 ms
T_{Kdec}	0.000036 second ≈ 0.036 ms
T_h	0.000011 second ≈ 0.011 ms
$T_{en/dec}$	0.000019 second ≈ 0.019 ms
T_{Ecc-M}	0.004382 second ≈ 4,3 ms
T_{fe}	0.002 seconds ≈ 2 ms

Table 4.3: Execution time notations in milliseconds

Scheme	USER	SERVER	Total cost
F. Wu et al [8]	**11 T_h**	**17T_h**	**28 T_h**
R. Amin et al [30]	**12 T_h**	**16 T_h**	**28 T_h**
R. Ali, et al [15]	**2$T_{en/dec}$ + 11 T_h**	**3 $T_{en/dec}$ + 16 T_h**	**5 $T_{en/dec}$ + 27 T_h**
S. Challa et al [20]	**2 T_{eccM} + 10T_h + T_{fe}**	**T_{eccM} + 4T_h**	**3 T_{eccM} + 14 T_h + T_{fe}**
X. Li. et al [22]	**T_{fe} + 2$T_{en/dec}$ +5T_h**	**6$T_{enc/dec}$+ 6 T_h**	**8 $T_{en/dec}$ + 11 T_h + T_{fe}**
Our scheme	**T_{fe} + 2T_{kenc} + T_{Kdec} +3T_h**	**T_{kenc} +2T_{kdec} + 3T_h**	**Tfe + 3 Tkenc + 3 Tkdec +6Th**

Table 4.4: computational cost comparison

Scheme	User cost	SERVER cost	Total cost
F. Wu et al [8]	**0.121**	**0.187**	**0.308**
R. Amin et al [30]	**0.132**	**0.176**	**0.308**
R. Ali, et al [15]	**0.159**	**0.233**	**0.392**
S. Challa et al [20]	**10.71**	**4.344**	**15.054**
X. Li. et al [22]	**2.093**	**0.18**	**2.273**
Our Scheme	**2.269**	**0.169**	**2.438**

Table 4.5: Execution time comparison

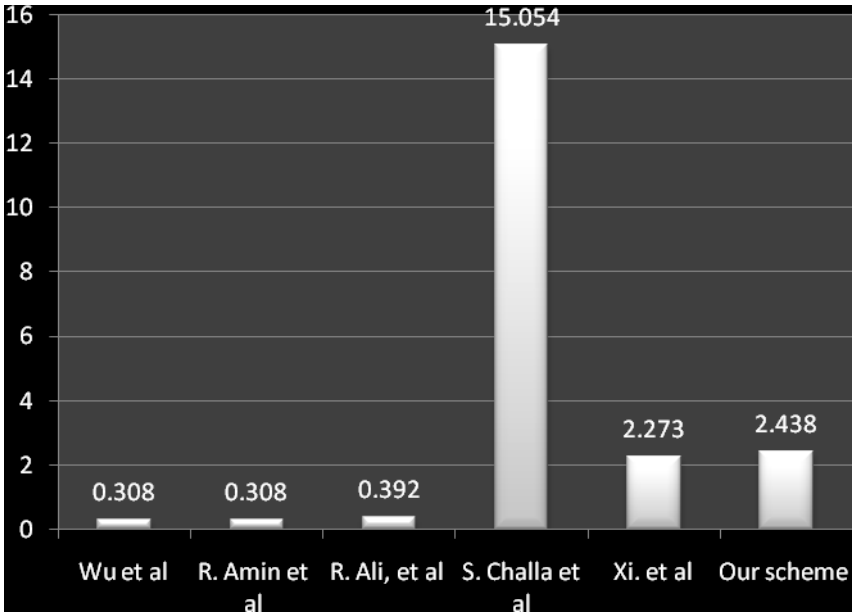

Figure 4.5: Comparison between total computational cost.

Scheme	**Communication cost**
F. Wu et al [8]	**2592 bits**
R. Amin et al [30]	**2272 bits**
R. Ali, et al [15]	**2016 bits**
S. Challa et al [20]	**1728 bits**
X. Li. et al [22]	**1312 bits**
Our scheme	**18504 bits**

Table 4.6: Comparison of communication cost

4.6.2. Computational analysis :

When it comes to computational cost of our proposed scheme, guarantees both lightweight and high security, when we talk about it is lightweight, this because it costs less than the scheme using ECC multiplication and hash functions of S. Challa et al, and it's 8 times less than this scheme, while it guarantees more than 128 bits of security against all known classical and quantum attacks [9]. It is 8 times more than the two first schemes they don't guarantee this level of security and even the last one of X. Li et al which also uses Biometric security does not.

4.6.3. Communication analysis :

Table 4.6 present the communication cost comparison. The communication cost of our scheme is more than or studied schemes because the length of ciphertext of Kyber is 768 bytes (6144 bits). However, our scheme can resist different possible attacks, including quantum attacks, than other ECC-based authentication schemes, such as Challa et al. [20] .

Conclusion

Conclusion

In this dissertation, we have studied the security in WBAN networks for healthcare applications. Our contribution is to propose a new authentication and key agreement protocol based on post-quantum PKE algorithm, called Kyber PKE scheme. To evaluate the performance of our proposed protocol, we implement different cryptographic primitives and compare the computational cost and communication cost with other existing WBAN-based authentication schemes. Our scheme is very fast than other ECC-based schemes and achieves different security requirements and resist several common attacks, including quantum attacks.

As future works, we will verify our proposed scheme by using formal tools, such as AVISPA tool. In addition, we will implement our scheme in IoT devices.

. ,

Bibliography

[1] . Abdelfettah Belghith , Negra, Rim, Imen Jemili . Wireless body area networks: Applications and technologies. 2017

[2] . Alam, Tanweer CMI Computing A Cloud, MANET and Internet of Things Integration for Future Internet. 2020 .

[3] . C. Wang, G. Xu and J. Sun, "An Enhanced Three-Factor User Authentication Scheme Using Elliptic Curve Cryptosystem for Wireless Sensor Networks," *Sensors*, vol. 17, no. 2, p. 2946, 2017.

[4] . Chen, M., Mau, D., Wang, X., & Wang, H. (2013). The virtue of sharing: Efficient content delivery in wireless body area networks for ubiquitous healthcare. In Communications Technology (ICACT). IEEE, 2013.

[5] . Cristoph paar, Jan Pelzl. Understanding Cryptography ,s.l. , Springers, 2010.

[6] . D. Mishra, and S. Mukhopadhyay A mutual authentication framework for wireless medical sensor networks J. Srinivas, journal of Medical System, 2017.

[7] . Elçin Önder , Alyssa Ungerer Measuring the Performance of Post-Quantum cryptography on embeded systems , WORCESTER POLYTECHNIC INSTITUTE, 2021.

[8] . F. Wu, X. Li, A. K. Sangaiah et al. A lightweight and robust two-factor authentication scheme for personalized healthcare. Futer generation computer system . 2017, Vol. 82.

[9] . Kyber , https://pq-crystals.org/kyber/ .

[10] . Malik, Bhavneesh, and V. R. Singh. "A survey of research in WBAN for biomedical and scientific applications." Health and Technology 3.3 (2013) .

[11] . Martin Noack Optimization of Two-way Authentication protocol in internet of things . s.l. : University of zurich , 2014 .

[12] . Mengxia Shuai, Bin Liu,Nenghai Yu. Lightweight and Secure Three-Factor Authentication Scheme for Wireless body Area network. School of Information Science and Technology, University of Science and Technology of China. 2019.

[13] . Movassaghi, Samaneh, et al. "Wireless body area networks: A survey." IEEE Communications surveys & tutorials 16.3 (2014): 1658-1686.

[14] . P. Kumar, S. Lee and H. Lee, "E-SAP: Efficient Strong Authentication Protocol for Healthcare Applications using Wireless Medical Sensor Networks," *Sensors*, vol. 12, no. 2, pp. 1625-1647, 2012.

[15] . R. Ali, A. K. Pal, S. Kumari, A. K. Sangaiah, X. Li, and F. Wu. s.l.An enhanced three factor based authentication protocol using wireless medical sensors : Journal of Ambient Intelligence and Humanized Computing, 2018.

[16] . RAMLI, Sofia Najwa, et al. A biometric-based security for data authentication in wireless body area network (wban). In: 2013 15th international conference on advanced communications technology (ICACT). IEEE, 2013. p. 998-1001.

[17] . Rhee, Woogeun, et al. "Low power, non-invasive UWB systems for WBAN and biomedical applications." International Conference on Information and

[18] . Ruben, Gunzales. Kyber , How does it work ?, 14 september 2021. https://cryptopedia.dev/posts/kyber/.

[19] . SHUAI, Mengxia, et al. Lightweight and secure three-factor authentication scheme for remote patient monitoring using on-body wireless networks. Security and Communication Networks, 2019, 2019.

[20] . S. Challa, A. K. Das, V. Odelu et al., "An efficient ECC based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," Computers and Electrical Engineering , vol 10 .

[21] . S. Kumari , O. Mir and J. Munilla "Efcient anonymous authentication with key agreement protocol for wireless medical sensor networks," Peer-to-Peer Networking and Applications, vol. 10.

[22] . X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan. new authentication protocol for healthcare applications using wireless medical sensors network with user anonymity. Security and communication networks . 2016, Vol. 9 .

[23] . Y. Deng, C. Chen, W. Tsuar, Y. Tang and J. Chen, "Internet of Things Based Design of a Secure and Lightweight Body Area Network (BAN) Healthcare System," Sensors, vol. 2919, 2017.

[24] . POLAT, Selahattin. Performance evaluation of lightweight cryptographic algorithms for internet of things security. 2019. Master's Thesis. Middle East Technical University

[25] . Pejman Niksaz, Young Researchers and Elite Club , Wireless Body Area Networks: Attacks and Countermeasures International Journal of Scientific & Engineering

Research, , Mashhad Branch, Islamic Azad University Volume 6, Issue 9, September-2015 .

[26] . Xiao, B., Yu, B., & Gao, C. (2007). CHEMAS: Identify suspect nodes in selective forwarding attacks. Journal of Parallel and Distributed Computing

[27] . Y. F. Chung and C. H. Liu, "Secure user authentication scheme for wireless healthcare sensor networks," Computers & Electrical Engineering, vol.

[28] . ZHANG, Junsong, et al. A Lightweight and Secure Anonymous User Authentication Protocol for Wireless Body Area Networks. Security and Communication Networks, 2021, 2021.

[29] . Zhiping, L., & Hui, L. (2010). Mobile jamming attack in clustering wireless sensor network. Paper presented at the Computer Application and System Modeling (ICCASM), 2010 International Conference on.

[30] . R. Amin, S. Islam, G. Biswas, M. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," Future Generation Computer Systems, vol. 80, 2015.