

# Quantum Secure Key Management System for healthcare



By

Hania Batool  
(Registration No: 00000329732)

Department of Information Security

Military College of Signals

National University of Sciences and Technology (NUST)

Islamabad, Pakistan

(2024)

# Quantum Secure Key Management System for healthcare



By

Hania Batool

(Registration No: 00000329732)

A thesis submitted to the National University of Sciences and Technology, Islamabad,

in partial fulfillment of the requirements for the degree of

Masters in

Information Security

Supervisor: Assoc. Prof.Dr. Shahzaib Tahir

Co-Supervisor: Asst. Prof. Dr. Fawad

Military College of Signals

National University of Sciences and Technology (NUST)

Islamabad, Pakistan

(2024)


**THESIS ACCEPTANCE CERTIFICATE**

Certified that final copy of MS Thesis written by Ns Hania Batool, Registration No. 00000329732, of Military College of Signals has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

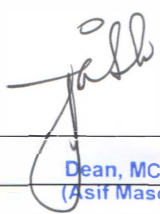
Signature:  \_\_\_\_\_

Name of Supervisor: Dr. Shahzaib Tahir

Date: \_\_\_\_\_

  
Signature (HOD): HoD  
Information Security  
Military College of Sigs

Date: \_\_\_\_\_

  
Signature (Dean/Principal) \_\_\_\_\_  
Date: 22/10/24 Brig  
Dean, MCS (NUST)  
(Asif Masood, Phd)

**NATIONAL UNIVERSITY OF SCIENCES & TECHNOLOGY**  
**MASTER THESIS WORK**

We hereby recommend that the dissertation prepared under our supervision by Hania Batool MSIS-19 Course Regn No 00000329732 Titled: "Quantum Secure Key Management System for healthcare" be accepted in partial fulfillment of the requirements for the award of MS Information Security degree.

**Examination Committee Members**

1. Name : Asst Prof Dr Fawad Khan

Signature: 

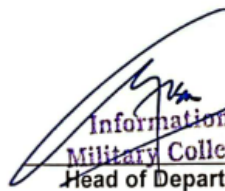
2. Name: Maj Bilal Ahmed

Signature: 

Supervisor's Name: Asst Prof Dr Shahzaib Tahir

Signature: 

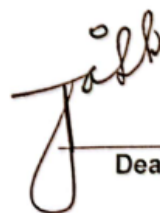
Date: \_\_\_\_\_

  
HoD  
Information Security  
Military College of Sigs  
Head of Department

\_\_\_\_\_ Date

**COUNTERSIGNED**

Date: 24/10/24

  
\_\_\_\_\_ Dean

### CERTIFICATE OF APPROVAL

This is to certify that the research work presented in this thesis, entitled "Quantum Secure Key Management System for healthcare," was conducted by Hania Batool under the supervision of Dr. Shazaib Tahir. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Military College of Signals, National University of Science & Technology Information Security Department in partial fulfillment of the requirements for the degree of Master of Science in Field of Information Security Department of information security National University of Sciences and Technology, Islamabad.

Student Name: Hania Batool

Signature: Hania Batool

Examination Committee:

a) External Examiner 1: Name Dr Fawad Khan. (MCS) Signature: Fawad Khan

b) External Examiner 2: Name Engr Bilal Ahmed. (MCS) Signature: Bilal Ahmed

Name of Supervisor: Dr. Shazaib Tahir


Signature: Shazaib Tahir

Name of Dean/HOD: Dr Muhammad Faisal Amjad

Signature: Dr Muhammad Faisal Amjad  
Information Security  
Military College of Sigs

## AUTHOR'S DECLARATION

I Hania Batool hereby state that my MS thesis titled Quantum Secure Key Management System for healthcare is my own work and has not been submitted previously by me for taking any degree from National University of Sciences and Technology, Islamabad or anywhere else in the country/ world. At any time if my statement is found to be incorrect even after I graduate, the university has the right to withdraw my MS degree.

Student Signature:   
Name: Hania Batool  
Date: 28-10-2024

## PLAGIARISM UNDERTAKING

I solemnly declare that research work presented in the thesis titled Quantum Secure Key Management System for healthcare is solely my research work with no significant contribution from any other person. Small contribution/ help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero-tolerance policy of the HEC and National University of Sciences and Technology (NUST), Islamabad towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS degree, the University reserves the rights to withdraw/revoke my MS degree and that HEC and NUST, Islamabad has the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized thesis.

Student Signature: \_\_\_\_\_

*Hania Batool*

Name: Hania Batool

Date: 20-10-2024

## DEDICATION

"In the name of Allah, the most Beneficent, the most Merciful"

I dedicate this thesis to my Parent, Brother, and teachers who supported me each step of the way.



# ACKNOWLEDGEMENTS

I would like to convey my gratitude to my supervisor, Dr. Shahzaib Tahir for his supervision and constant support. His invaluable help of constructive comments and suggestions throughout the experimental and thesis works are major contributions to the success of this research. Also, I would thank my committee members; Maj Bilal Ahmed and Dr. Fawad Khan for their support and knowledge regarding this topic.

I also want to thank all the school's faculty and staff members for creating suitable academic conditions and providing all the required means. .

Last but not the least, special thanks to all my family, friends and colleagues for the constant support they have provided me during the conduction of this project.

# Contents

|  |             |
|--|-------------|
| <b>ACKNOWLEDGEMENTS</b>  | <b>vii</b>  |
| <b>LIST OF TABLES</b>  | <b>x</b>    |
| <b>LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS</b>                     | <b>xii</b>  |
| <b>ABSTRACT</b>  | <b>xiii</b> |
| <b>1 INTRODUCTION</b>  | <b>1</b>    |
| 1.1 Background . . . . .   | 1           |
| 1.2 Motivation and Contribution . . . . .                              | 2           |
| 1.3 Research Objectives . . . . .                                      | 2           |
| 1.4 Thesis Organization . . . . .                                      | 3           |
| <b>2 LITERATURE REVIEW</b>   | <b>6</b>    |
| 2.1 Healthcare and the Internet of Things . . . . .                    | 6           |
| 2.2 Body Sensors and Remote Monitoring . . . . .                       | 9           |
| 2.3 Wearables Devices . . . . .  | 10          |
| 2.4 Patient Data on Cloud Concerns . . . . .                           | 11          |
| <b>3 PRELIMINARIES</b>   | <b>17</b>   |
| 3.1 Lattices Based Cryptography . . . . .                              | 17          |
| 3.2 Public Key Encryption, Post-Quantum Cryptography, and Kyber . . .  | 21          |
| 3.2.1 Introduction . . . . .   | 21          |
| 3.3 Kyber by Example . . . . .   | 24          |
| 3.3.1 Encryption Process . . . . .                                     | 25          |
| 3.3.2 Decryption Process . . . . .                                     | 26          |
| 3.4 Feature Extraction and Generation of Cancelable Biometric Template | 27          |
| 3.4.1 Use of Physiological Patient Data . . . . .                      | 27          |

|          |  |           |
|----------|--|-----------|
| <b>4</b> | <b>PROPOSED HOSPITAL KEY MANAGEMENT SYSTEM</b>   | <b>38</b> |
| 4.1      | System Component . . . . .   | 38        |
| 4.1.1    | Patient Sensor - Wearable Device . . . . .   | 38        |
| 4.1.2    | Hospital Server . . . . .  | 38        |
| 4.2      | Process Flow . . . . .   | 38        |
| 4.3      | Secure Channel Establishment between Patient Sensor device and Hos-<br>pital Server and Doctor . . . . . | 41        |
| 4.3.1    | Mutual Authentication: . . . . .   | 41        |
| 4.3.2    | Session Key Generation . . . . .   | 43        |
| <b>5</b> | <b>ALGORITHMS</b>  | <b>46</b> |
| 5.1      | Kyber Key Generation Algorithm . . . . .   | 49        |
| 5.2      | Kyber Encapsulation Algorithm . . . . .  | 49        |
| 5.3      | Kyber Decapsulation Algorithm . . . . .  | 50        |
| 5.4      | Algorithm: Session Key Derivation . . . . .  | 51        |
| <b>6</b> | <b>ANALYSIS OF THE PROPOSED SYSTEM</b>   | <b>52</b> |
| 6.1      | Security Analysis . . . . .  | 52        |
| 6.2      | Performance Analysis . . . . .   | 53        |
| <b>7</b> | <b>SUMMARY OF RESEARCH WORK</b>  | <b>56</b> |
| <b>8</b> | <b>CONCLUSION</b>  | <b>58</b> |
| 8.1      | Conclusion . . . . .   | 58        |
| 8.2      | Future Work . . . . .  | 59        |
|          | <b>References</b>  | <b>60</b> |
| <b>A</b> | <b>CODE IMPLEMENTATION</b>   | <b>66</b> |
| A.0.1    | Loading and Preprocessing the ECG Signal . . . . .   | 66        |
| A.0.2    | Plotting the ECG Signals . . . . .   | 67        |
| A.0.3    | R-Peak Detection and Threshold Calculation . . . . .   | 67        |
| A.0.4    | Feature Detection: P-Waves and T-Waves . . . . .   | 67        |
| A.0.5    | Plotting Detected Features . . . . .   | 68        |

# List of Tables

|     |  |    |
|-----|--|----|
| 2.1 | Literature Review . . . . .                        | 14 |
| 2.2 | Literature Review . . . . .                        | 15 |
| 2.3 | Literature Review . . . . .                        | 16 |
| 3.1 | LWE vs RLWE vs MLWE: A Comparison . . . . .        | 22 |
| 3.2 | Kyber Security Levels . . . . .                    | 24 |
| 3.3 | Feature Extraction Algorithm Comparison . . . . .  | 33 |
| 3.4 | ECG data source and its characteristics: . . . . . | 35 |
| 6.1 | System Specification . . . . .                     | 53 |
| 6.2 | Performance Table . . . . .                        | 53 |

# List of Figures

|     |  |    |
|-----|--|----|
| 2.1 | IOMT Environment . . . . .               | 9  |
| 2.2 | Wearable Sensor Types . . . . .          | 11 |
| 2.3 | Healthcare Data Breach by Year . . . . . | 13 |
| 3.1 | Feature Extraction from ECG . . . . .    | 28 |
| 3.2 | Filtered ECG Signals . . . . .           | 35 |
| 3.3 | Detected R Peak . . . . .                | 36 |
| 3.4 | Detected Peaks . . . . .                 | 36 |
| 3.5 | Cancelable Template Generated . . . . .  | 37 |
| 4.1 | Sequence Flow Diagram . . . . .          | 45 |
| 5.1 | KeyGeneration . . . . .                  | 47 |
| 6.1 | Kyber variant Comparison . . . . .       | 54 |

# ABBREVIATIONS , SYMBOLS AND ACRONYMS List

|      |                                   |
|------|-----------------------------------|
| PUFF | Physiological Unclonable Function |
| HRNG | Hardware Random Number Generator  |
| TPM  | Trusted Platform Module           |
| SMA  | Secure Mutual Authentication      |
| KEM  | Key Encapsulation Mechanism       |
| KMS  | Key Management System             |
| LWE  | Learning with errors              |
| MK   | Master Key                        |
| TAK  | Temporary Access Key              |
| DoS  | Denial of Service                 |
| MITM | Man-in-the-Middle                 |
| TPM  | Trusted Platform Module           |
| HRNG | Hardware Random Number Generator  |
| HS   | Hospital Server                   |
| SVP  | Shortest Vector Problem           |
| CVP  | Common Vector Problem             |

# Abstract

This paper introduces a Quantum-Resistant HKMS which addresses the needs of patients who want to have more control over their cryptography keys to mitigate the insider dangers. The KMS traditionally refers to centralized Key Management Systems where the centralized structure has authority over the master keys and in many cases, has numerous powers in terms of security which in most cases can lead to the introduction of new sources of weakness, and particularly the so-called insider threats. Our approach alleviates these concerns by removing reliance of central key management from the system; patients actually create and can manage their keys on their own.

In our system, the keys are generated from the patient's physiological data, for instance, ECG signals, which implies that the key generation procedure remains under the control of the patient. It greatly minimizes the chance of key exposure to any central authority and improves the protection of the communication links between the patient wearable sensors and the system.

Therefore, by using the quantum-resistant cryptographic methods for integration, our proposed solution minimizes the vulnerability of threats, including threats from a quantum computing system. This decentralized approach guarantees that even in cases where a centralized health data system is implemented, the patients' most secure cryptographic keys remain under their sole control eliminating the insider threat factor while promoting secure transfer of health data. The proposed system provides a balanced, yet decentralized, approach to securing patient information, offering strong protection against current and future security challenges.

**Keywords:** KMS; Health Data, Data Privacy, remote monitoring, wearable body sensors, PHR.

# Chapter 1

## INTRODUCTION

### 1.1 Background

As the digital healthcare space evolves by leaps and bounds, so does our need to protect more patient data. Many medical organizations have moved towards digitalizing their way of maintaining patient health data so this data is stored on cloud. The cloud storage of records facilitates the easy sharing of patient data amongst several stakeholders, including the patient, physicians, nurses, and other healthcare providers involved in different phases of the patient's treatment to solicit feedback. Healthcare systems have a greater need for protective solutions that are resilient against emerging security threats, such as quantum computing, and we can expect the usage of remote monitoring devices, such as wearable body sensors, to be more widely used. Traditional key management systems (KMS), which are typically based on centralized control, show significant weaknesses with respect to insider threats. Furthermore, these systems centralize the generation and storage of cryptographic keys, which means that some party with good intentions within a hospital could have unauthorized access to sensitive health data.

This research proposes the development of a quantum-proof health key management system (HKMS) to combat these difficulties by removing control over keys by one party and thus reducing susceptibility to patient data security threats. Using unique physiological data (e.g., electrocardiogram - ECG signals) from patients, among others, to produce cryptographic keys[1][2][3]. This research proposes a solution to give control to patient on its own data. First, by allowing patients to receive and handle their master keys independently, the system reduces its dependence, lowering an innate risk of inner threats. World is facing threat of quantum computing. Existing HKMS are vulnerable to it. We are considering this threat and make our system quantum resistance by generating cryptography keys using kyber.



## 1.2 Motivation and Contribution

The aim of this study is to investigate the feasibility and necessary conditions for implementing the system within the prevailing setting of healthcare data management. The HKMS has been proposed to provide security for communication channels between the wearable sensor and KMS as well as handing ownership of PHR back to patients and make this channel quantum resistant. This is a big leap toward securing sensitive data today with quantum computing on our collective horizon, which could easily break traditional encryption.

## 1.3 Research Objectives

The focus of this research encompass the design and implementation of a Post-Quantum Cryptography-based Secure Keys management system for the protection of sensitive medical data within hospital environments against future quantum threats. This overarching goal is supported by several specific objectives:

- **Implement Quantum-Resistant Cryptography for Secure keys Management Solution:** To use a Kyber based key encapsulation mechanisms (KEM), which is a post quantum cryptographic algorithm, to generate secure mutual channel between the patient, doctor and the hospital server. The intention is to make the system secure from the attacks of both the classical and the quantum computing.
- **Generate Kyber Key Pairs Using Patient Physiological Data:** To incorporate Physiological Unclonable Functions for creating Kyber key pairs based on patients' unique physiological characteristics every time the session is held. This means that cryptographic keys will always be linked to the specific attributes of the patient and therefore the system will not be easily susceptible to impersonation thus improving on the security.
- **Ensure Data Confidentiality and Controlled Access:** In order to achieve the patient-controlled access mechanism that allows patient to control decision on who should have access to the data in real-time. This objective helps the patient to have full control of his/her medical records, including authorizing any third party to access his/her records even in collaborative settings.

## 1.4 Thesis Organization

The Thesis structured as follow:

Chapter 2 discusses prior related research used in develop the thesis of the paper through the consideration of the effects that IoT brings to the healthcare sector. It discusses the main threats and attacks to which IoT devices used in health care settings are vulnerable and studies the countermeasures that researchers have suggested. This chapter focuses on how the IoT is revolutionizing the management of healthcare facilities, the threats that IT brings about, and the different measures that continue to be put in place to improve on security and safeguard health information.

Chapter 2 discusses prior related research used in develop the thesis of the paper through the consideration of the effects that IoT brings to the healthcare sector. It discusses the main threats and attacks to which IoT devices used in health care settings are vulnerable and studies the countermeasures that researchers have suggested. This chapter focuses on how the IoT is revolutionizing the management of healthcare facilities, the threats that IT brings about, and the different measures that continue to be put in place to improve on security and safeguard health information.

Chapter 2 discusses prior related research used in develop the thesis of the paper through the consideration of the effects that IoT brings to the healthcare sector. It discusses the main threats and attacks to which IoT devices used in health care settings are vulnerable and studies the countermeasures that researchers have suggested. This chapter focuses on how the IoT is revolutionizing the management of healthcare facilities, the threats that IT brings about, and the different measures that continue to be put in place to improve on security and safeguard health information.

Chapter 2 discusses prior related research used in develop the thesis of the paper through the consideration of the effects that IoT brings to the healthcare sector. It discusses the main threats and attacks to which IoT devices used in health care settings are vulnerable and studies the countermeasures that researchers have suggested. This chapter focuses on how the IoT is revolutionizing the management of healthcare facilities, the threats that IT brings about, and the different measures that continue to be put in place to improve on security and safeguard health information.

Chapter 3 proposes the conceptual framework of the Health Key Management System (HKMS) that will be developed in this research. It starts with lattices, how they empower post-quantum cryptography mainly through the use of difficult problems such as the Learning With Errors (LWE). Kyber—one of the

world's most efficient and secure lattice-based post-quantum key encapsulation mechanism (KEM) is presented in this paper, especially concerning healthcare facilities. Feature extraction from physiological data like ECG for purpose of generating cryptographic keys is also described in the chapter. In order to prevent the leakage and misuse of such data, cancelable templates are used, which allow one to transform physiological characteristics into non-convertible and renewable ones, preserving the initial templates and increasing the degree of protection in general.

Chapter 4 outlines the proposed quantum-secured Key Management System (KMS) designed specifically for healthcare applications. This scheme leverages post-quantum cryptography, particularly the Kyber algorithm, to ensure resilience against future quantum threats. The system enables patients to generate and control their own cryptographic keys using physiological data, such as ECG signals, as a unique biometric source. By integrating Post Quantum algorithm with feature extraction techniques, the system offers enhanced security, minimizing reliance on central authorities while ensuring that only authorized individuals can access sensitive health data. The use of cancelable templates further protects biometric information, allowing for revocation and regeneration of keys if needed, ensuring the long-term security of patient data in a quantum-secured environment.

Chapter 5 details the algorithms implemented in the development of the proposed Key Management System (KMS). It presents the step-by-step process for generating and managing cryptographic keys using the Kyber post-quantum algorithm. The chapter explains how physiological data is collected, features are extracted, and cancelable templates are created for secure key generation. It also outlines the integration of these steps into the overall system, ensuring that the keys remain quantum-resistant and protected against unauthorized access. The algorithms ensure that the system is secure, efficient, and capable of supporting the healthcare environment's stringent data protection needs.

Chapter 6 presents the analysis of the proposed Key Management System (KMS). It evaluates the system's performance in terms of security, efficiency within a healthcare environment. The chapter analyzes the system's resilience to quantum attacks, highlighting how the use of the Kyber algorithm and lattice-based cryptography ensures robust protection of sensitive patient data. The analysis also includes a discussion on the system's computational overhead and its suitability for real-world healthcare applications.

Chapter 7 summarizes the proposed quantum-secured Key Management System (KMS) for healthcare. The system enhances security using the Kyber algorithm for protection against quantum and classical threats. It generates cryptographic keys from physiological data, like ECG signals, giving patients control

over their data. The system minimizes reliance on central authorities, mitigates insider threats, and secures sensitive health data, offering a robust solution for healthcare security.

Chapter 8 concludes the document by summarizing the key findings of the proposed quantum-secured Key Management System (KMS) and its effectiveness in enhancing healthcare security through post-quantum cryptography and biometric key generation. It also identifies future work areas and optimizing performance in real-world settings. The chapter emphasizes the need for ongoing research to tackle emerging security challenges posed by advancing quantum technology.

# Chapter 2

## LITERATURE REVIEW

### 2.1 Healthcare and the Internet of Things

Security and privacy are paramount in the healthcare systems mainly because healthcare providers are entrusted with the responsibility of handling the personal information of patients regarding their tests, insurance, medical history, and billing information among others. Such systems primarily dealing with large databases containing personal information are most vulnerable to hacking and data theft. In this opinion, the author emphasizes that the threat of cyberattacks has recently manifested and become a major concern for the healthcare industry all over the world. Data breaches in the healthcare sector were reported to be at about 10% in 2020 and affected over 25 million patient records across the globe (Hernandez, 2021).

IoT in healthcare systems involve the employment of the IoT devices and technologies within the health care delivery services with the aim of increasing the quality of patients' health through constant monitoring and processing of data through technologies such as; Such systems are intended to augment patients' well-being and quality of care as well as to decrease costs by tracking health conditions via wearable, implantable, and smart homes. These devices monitor various health parameters including pulse rate, blood pressure, and glucose level transmitting the data to control servers and clouds for analysis and decision making [4]. Some of the advantages include cutting down of hospital re admissions, early signs of poor health and development of individualized treatment plans. However the use of IoT in healthcare brings many security and privacy concerns. IoT devices provide easy entrance for hackers, hence the integrity and privacy of patient's data is at risk. To eliminate these risks, adequate security and privacy mechanisms have to be adopted by the healthcare organizations in order to safeguard patients' information and maintain the integrity of the systems.

Bringing IoT devices into the health care facilities poses a specific security and privacy risks [5]. These devices can also be hacked making information stored in them

compromised and open to external access. Moreover, management of patient information is also an issue of privacy as patients are also willing to reveal information relating to their health. To address these risks, healthcare organizations have to ensure adequate security and privacy controls such as encryption, access, and authentication as well as data anonymization. Although IoT-based systems can lead to better patients' conditions, higher efficiency of treatment, and lower costs, these questions need to be solved to ensure the security of patients' information and the stability of the system. [6] 36% of the healthcare facilities have informed that they are experiencing more of medical complications as an outcome of the attack. A new statistics show that employee recklessness is responsible for 61% of health data violations.

A number of hospitals have been attacked by ransomware that was 1 in 42 healthcare organizations during the third quarter of the year 2022. Moreover, it is elicited that 92.7% of the healthcare firms have been attacked by data breach in the last three years. This points to the fact that the problem is systemic, meaning that it cuts across most health care facilities and has brought significant financial and operational consequences.

Losses pertaining to healthcare data breaches are relatively high with an average of \$4. 24 million per incident, that is much higher than the cross-industry average. Ransomware attacks have been reported to have cost the healthcare sector an amount of \$157 million from the year 2016 up to now and average cost per breach is \$10. 10 million. These financial losses show the critical situation of health care organizations due to data breaches.

One of the most significant information security risks that companies come across is Employee negligence. While organizations aim to secure personal information, careless actions can compromise the data including acting reckless in handling it, setting insignificant passwords, or not following security measures. Such a negligence can result in an inadvertent leakage of information, loss of confidential data and an organization's exposure to attacks such as cyber raids. Often, such oversights give the attackers basic entry points into secure systems, which can exponentially increase the extent of the problem. The IoMT has become a game changer in healthcare through offering real time data acquisition and supportive patient management through interconnected Medical Things. But this brings with it some problems as well. Healthcare organizations collect, process, and store large amounts of personally identifiable information on network servers to provide uninterrupted access and enhance patient care, which is convenient but not secure. Taking into account the given case that smart devices such as smartphones are the most common means of privacy violations due to their insecurity, insecure applications, and human mistakes. Such problems may result in violation of privacy and disclosure of critical information. Employee threats can exacerbate the risk of protected health information loss to data, theft, or unauthorized disclosure; planned or unintended. The financial consequences are rather dramatic since a full patient record may cost hundreds of dollars on the market [4]. According to literature,

the healthcare industry continues to be one of the worst hit by such breaches and thus the call for smarter security features and monitoring of health-related information [7] [8].

There has been several major one in recent times. For example, OneTouchPoint has reported the breach that occurred in July of 2022 which affected more than 1 million people. The breach in the Shields Health Care Group was noted in March 2022, and it impacted more than 2 million records. Another case was the Novant Health that experienced misconfiguration of data which resulted into leakage of a large number of approximately 1362296 records. Such incidents show the number and the extent of data breaches that occur in the healthcare industry.

Nonetheless, the healthcare continues to remain an attractive target for cyber attackers given the vast amounts of data it possesses. These risks can be prevented through the enhancement of organizational security, carrying out of risk analysis frequently, and continuous adherence to standards especially HIPAA and GDPR. The ever increasing number and financial impact of the breaches make it evident that there is a dire need to implement strict security that will help prevent leakage of patients' data [9]. We can now look at some of attack that involves IOT in healthcare [10]. One of them is Selective-forwarding attack [11] is where there are bad nodes which forward packets only to undesirable destinations or do not forward at all leading to DoS conditions. For instance, this can make the system block send out actionable notifications, this being in instances like in the case of a sensor sending a signal of a heart attack. Sinkhole attacks [12] involve an attacker creating an apparently advantageous routing path that when other nodes in the vicinity send their traffic through the supposed preferred routing path end up routing their traffic through the said malicious node. This attack may not disrupt the network operations at the initial instance and is even more lethal when combined with other forms of attacks such as selective-forwarding in which attackers can block the flow of sensitive patient information intended for other legitimate healthcare organizations. Jamming [13] is the process of transmitting noise signals that disrupt the frequencies used by IoT devices to communicate thus denying data exchange. Flooding attacks [13] target the depletion of the target's resources including battery, processing power, bandwidth or memory through the flooding of connection requests interfering with the constant flow and logging of sensor data. Last, there is the phishing attack in which the attacker aims at using deception to make a user reveal information that is personal, such as Wi-Fi connections to enable the attacker to gain unauthorized access to the IoT resources to compromise the security data accumulated by the environmental nodes. Many authentication protocol and security solutions are proposed by researchers to secure remote monitoring and telecare. An access control and key establishment mechanism based on ECC and two factors was proposed by Xu et al [14]. But Islam and Khan (2014) [15] cryptanalyzed Xu et al key agreement protocols which were proposed to be implemented in telecare medicine information systems (TMIS). They pointed potential security issues in the protocols,

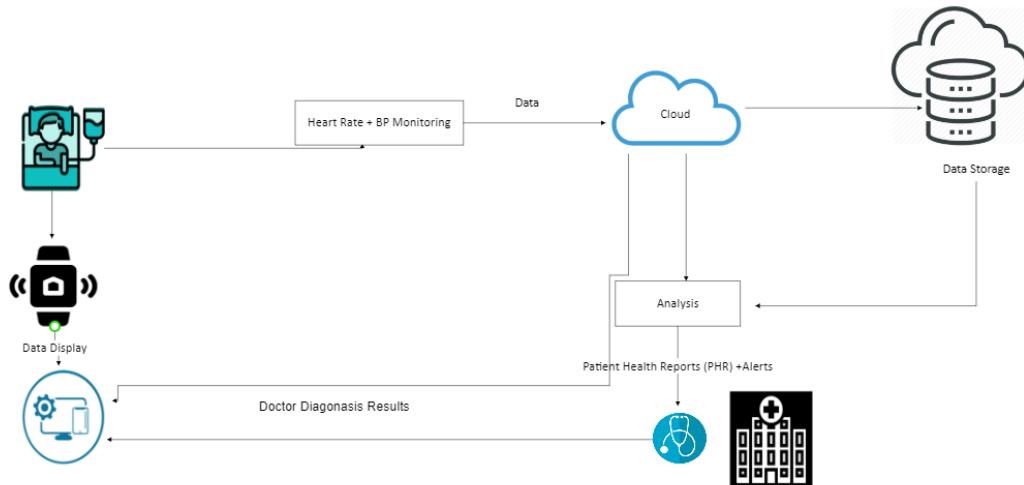


Figure 2.1: IOMT Environment

such as vulnerability to different types of attacks (e.g., impersonation, replay attack, man-in-the-middle) and fails in completing mutual authentication.

They also presented improved scheme to potentially covers the weaknesses in Xu et al scheme. [16] found that the Islam and Khan scheme is also vulnerable to impersonation and the man-in-the-middle attack. They also provided an improved two-factor authentication scheme. Chaudhry et al.'s approach is vulnerable to man-in-the-middle attacks, offline password guessing attacks, and user/server impersonation attacks for TMIS (Telecare Medical Information Systems), as pointed out by Qiu et al [17]. To address these problems, they subsequently suggested a mutual authentication system based on elliptic-curve cryptography.

## 2.2 Body Sensors and Remote Monitoring

Figure 2.1 shows how a patient is monitored from remote.

As an alternative to costly and unwelcome healthcare institutions like hospitals or nursing homes, remote healthcare monitoring lets people stay healthy in their own homes [18][19]. After the recent covid 19 pandemic, the trend of remote patient monitoring is increasing [20]. This makes it a productive and affordable replacement for clinical on-site monitoring. The concept of "Hospital at Home," or remote patient monitoring, presents an appropriate way to deal with hospital capacity issues. This approach lessens the demand on healthcare facilities and eliminates the need for extended hospital stays by enabling patients to monitor and manage their health conditions continuously from the convenience of their own homes. Hospital at Home models also offer personalized care, reduce the possibility of infections acquired while in the hospital, and



enhance patient outcomes. By providing care in a more comfortable and relaxed setting, this creative method not only maximizes the use of resources in hospitals but also improves patient satisfaction overall [21]. Investigating the vital physiological signals and activities of patients could also be a viable diagnostic aid to healthcare providers if such systems are built with non-invasive, unobtrusive wearable sensors that monitor them in real-time from distant facilities [22]. Remote monitoring systems are also gaining ground in the field of continuous care and surveillance, particularly for elderly patients. These systems are especially useful for elderly patients, many of whom have chronic medical conditions or mobility problems that make frequent hospital visits difficult. Healthcare providers can monitor a patient's condition by sending alerts when vital signs are out of range or detecting adverse trends while the patient is at home, using wearable devices and other remote technologies that provide real-time data. Using body sensors, it is possible to measure and transmit physiological data, including blood pressure, body temperature, heart rate/pulse rate, respiration rate, and blood oxygen saturation [23], [24].

For postoperative patients, remote monitoring provides a means of tracking recovery during the crucial period after surgery, reducing complications while allowing rapid intervention if things go wrong. This not only increases patient safety but also offers reassurance and support during their recovery process, which can lead to better overall outcomes [25] [26].

Patient monitoring systems traditionally employed wired sensors connected to computers inside hospitals. The disadvantage of these systems was that they restricted patient's mobility [20]. As medical sensors are handling patient health data, ensuring communication is a priority. Patients' privacy can be breached and opponents can manipulate or alter true health records in the field without solid security functionalities, which then leads to incorrect diagnosis of ailments [27].

## 2.3 Wearables Devices

Wearable technology refers to devices that are worn on the human body, weaved into fabrics, or implanted into the skin. Such devices can comprise accessories, implants or the skin-mounted sensors or even smart garments and they can be used in various domains of application including fashion, fitness, health, games and sports. Pervasive, portable, and without stands or need for hand interaction, wearables feature microprocessors and are capable of sending and receiving Internet data.

The first significant step towards wearable devices was made with the help of fitness bands or activity trackers which started becoming popular quite soon after their emergence. These devices later on advanced with features such as screens, wrist watches and an integration of with mobile applications. Once people discovered the benefits of this technology, they started searching for various ways to apply it to different

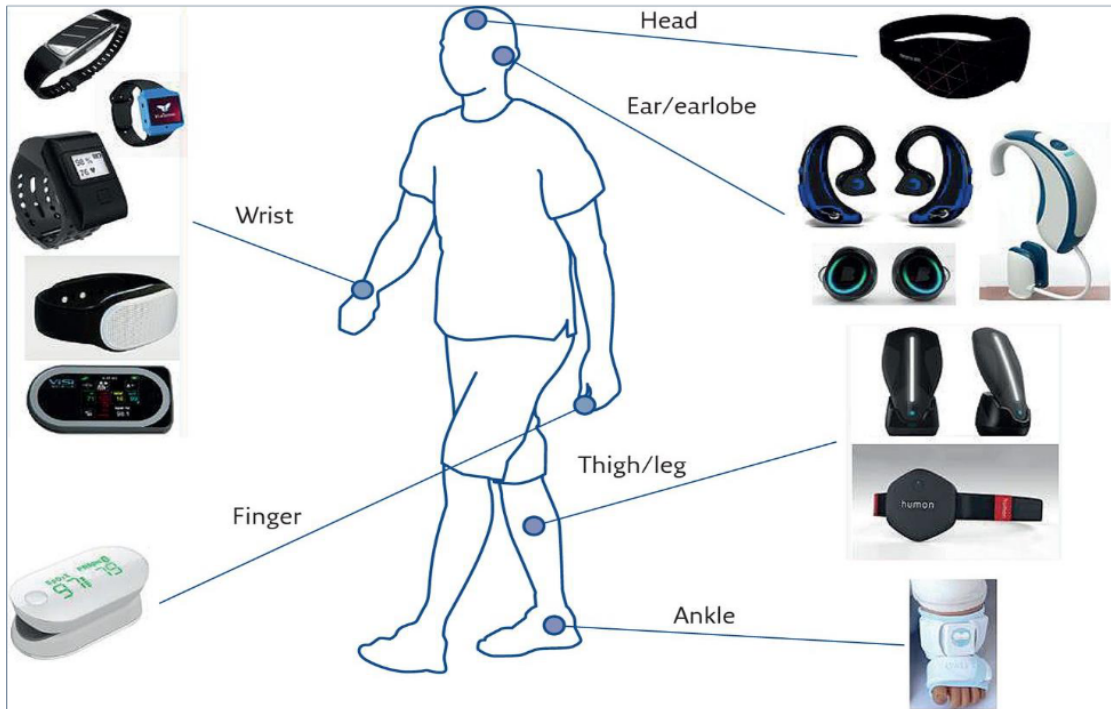


Figure 2.2: Wearable Sensor Types

industries, which in turn created a vast number of digital products based on wearable to bring the best user experiences and actual utilities.

The fig 2.2 shows different types of wearable:

## 2.4 Patient Data on Cloud Concerns

### Healthcare Data breach statistics at a glance (2023-2024)

Modern developments in healthcare have been involving a variety of threat points associated with the data breaches and cybersecurity issues. In 2023 and 2024, various statistics highlight the severity and impact of these breaches: In 2023 and 2024, various statistics highlight the severity and impact of these breaches:

#### General Trends and Impact:

[28][29] In healthcare, data breaches have also somehow declined slightly with an average drop by 48% based on reports from HIPAA. However the sector has not moved far from worse off and still faces serious challenges. Data show that ransomware attacks have impacted the medical treatment of patients in 36% of the institutions and only a fraction of 4-7% of the healthcare IT expenses are spent on cybersecurity. The study

offers a shocking revelation that negligent workers account for 61% of all the security breaches and this calls for better training and stringent measures. However, 93% of the healthcare organization has been impacted with at least one data breach in the last three years with more than 57% organizations had faced breach more than five times in three years.

### **Statistical Highlights:**

**Breach Probability:** According to the data obtained in 2023, it has increased by 75 per cent. Two percent odds of a breach that compromises 100,000 to 5 million records; and a 6 percent likelihood of a bare minimum of a 5-million record leakage.

**Ransomware Incidents:** Specifically, 2.41% of the healthcare organizations made it on the list of institutions that fell victim to ransomware attacks in the third quarter of 2022.

**Exposed Records:** Some attackers compromise more than 42 million records between March 2021 and February 2022, while most identity theft come from stolen hospital records with the proportion of 95%.

**Increased Attacks:** It has been found that the frequency of cyber-attacks has risen by 60 percent from the last year with approximately, 1,426 attacks per week. The industry registered a 42% rise in data breaches since 2020, according to the latest Deloitte report.

### **Types and Costs of Data Breaches:**

The major types of incidents reported in the Healthcare Industrial are phishing, ransomware and business email compromise. According to the research, 88% of the healthcare workers fell victim of phishing, while ransomware was most destructive having attacked 74% of the hospitals. The instances of business email compromises have risen sharply and the healthcare sector has been worst hit with a 473% rise in email fraud.

The fig 2.3 tells the Data Breaches from 2009 to 2024.

### **Notable Incidents:**

Several significant breaches occurred recently:

- **OneTouchPoint:** Due to unauthorized attempts made at accessing the servers, more than 1 million people were impacted.
- **Shields Health Care Group:** One of the largest data breaches of 2022, which affected more than 2,000 000 people and which involves personal and medical data.
- **Novant Health:** Meta pixel code misconfiguration caused the unintended exposure of PHI for 1. 36 million individuals.

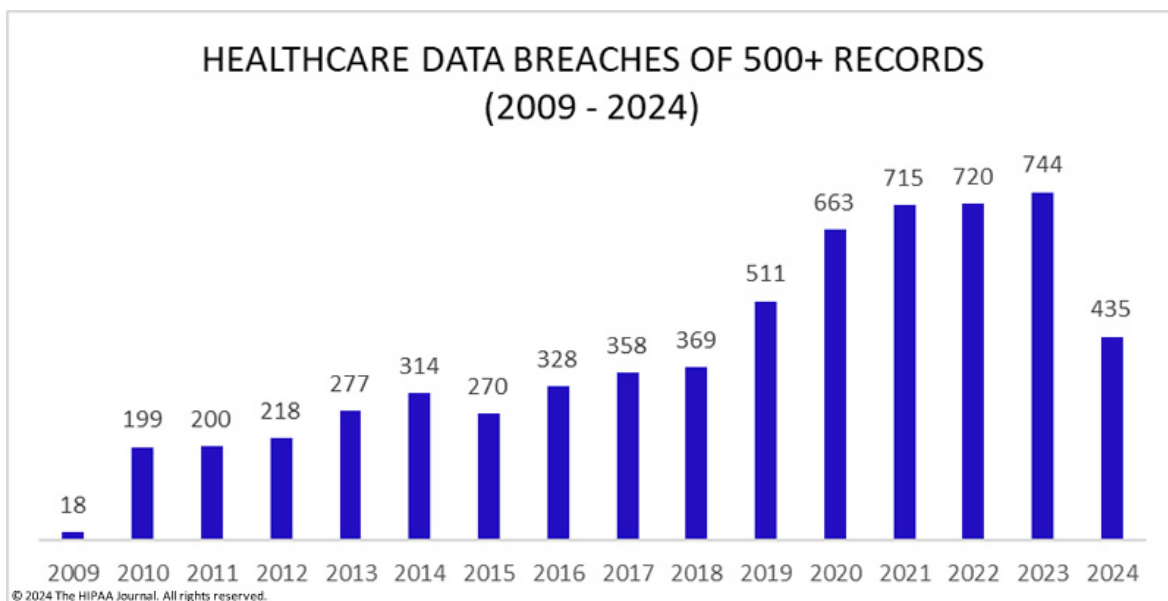


Figure 2.3: Healthcare Data Breach by Year

- Broward Health and Baptist Medical Center: These two suffered massive attacks that compromised the data of 1.35 million and 1.24 million individuals respectively.

#### Cost of Breaches:

According to the survey the average expenses in health care due to data breach is \$10.10 million, which is much above the general average of \$9.23 million. Healthcare breaches also remain to be among the costliest with each record averaging at \$408, the highest across all industries. Ransomware attacks alone have taken \$157 million since 2016 impacting the healthcare industry severely, and with an approximate annual loss from stolen PHI valued around \$7 billion in the U.S. on average.

As mentioned above, the majority of data breaches in healthcare is caused by carelessness and lack of awareness of the doctors and the employees of the hospitals. In order to prevent such problems, certain measures should be taken as follows: a. Patient control – that means patients should have full control over data that are created and used in their treatment. b. Secure communication – the communication channels should be as secure as possible. Thus, it is possible to minimize the exposure of breaches with proper data governance, and increase the overall level of cybersecurity as a constant threat to the patients' records should be acknowledged and discussed in more detail.

We summarize our research in the in Table 2.1

| Author                   | Contribution  | Limitation   | Quantum Secure  |
|--------------------------|---|--|---|
| Marcus de Ree et al [30] | Devise Key management Framework for Remote Monitoring which provides point point communication security                   | Reliance on KDC and trust in hospital technical employee   | Use of Symmetric Cryptography makes it quantum resistance if adequate key length is used. |
| Turkanovic et al [31]    | Proposed a key authentication and establishment scheme for WSN  | Vulnerable to smart card stolen and impersonation attack   | No  |
| Amin et al [32]          | Analyzed Farash et al proposed scheme and proposed remediation. They proposed anonymity multifactor authentication scheme | Vulnerable to replay attack, smart card stolen attack and does not provide untracibility of the user |   |

**Table 2.1.** Literature Review

| Author                 | Contribution  | Limitation   | Quantum Secure |
|------------------------|---|--|----------------|
| Pal et al[33]          | Proposed access control architecture and use symmetric cryptography for authentication                                      | Not applicable to implement proposed fine grained access control method  | may be         |
| Alabdulatif et al.[34] | Develop a novel secure computing platform for healthcare using fully homomorphic encryption under the Edge of Things (EoT). | Computation overhead Because of the use of fully homomorphic encryption  | No             |
| Sharma et al[35]       | Proposed lightweight authentication scheme for remote patient monitoring  | Vulnerable to various types of attacks like priveleged insider attacks, password guessing attacks, impersonation attacks | No             |

**Table 2.2.** Literature Review

| Author                | Contribution  | Limitation   | Quantum Secure |
|-----------------------|---|--|----------------|
| Chandrakar et al [36] | Cloud-based healthcare system   | Prone to unlinkability, non-repudiation, and impersonation attacks         | No             |
| Zhou et al. [37]      | Presented a novel authentication scheme for IoT-based architectures combined with cloud servers | Vulnerable to user impersonation, replay, privileged-insider, MITM attacks | No             |
| Farash et al [38]     | Proposed secure authentication, key establishment, and communication scheme for WSN             | Vulnerable to replay, impersonation, forgery attack                        | No             |

**Table 2.3.** Literature Review

# Chapter 3

## PRELIMINARIES

### 3.1 Lattices Based Cryptography

Over recent years, cryptography has turned to the complexity of the problems regarding lattices which is used mainly in the development of post-quantum cryptographic schemes. Some of the crucial cryptographic challenges that come under this domain are known as Learning With Errors (LWE), Ring-Learning With Errors (RLWE), and Module-Learning With Errors (MLWE). All of these problems constitute the foundation of diverse cryptographic protocols that are meant to protect against quantum adversaries with different levels of relative efficiency and usability.

**Lattices Problems LWE, RLWE and MLWE:** LWE, RLWE, and MLWE are introduced in this chapter along with the differences, similarities and trade-offs between these three different variants of LWE in terms of security and efficiency. We also talk about their application to the lattice-based cryptography and to post-quantum security.

**Learning With Errors (LWE):** The LWE problem can be defined as follows:

- Let  $\mathbf{A}$  be a random matrix over a finite field.
- The secret vector  $\mathbf{s}$  and the error vector  $\mathbf{e}$  are chosen.
- The goal is to solve for  $\mathbf{s}$  given  $\mathbf{As} + \mathbf{e} = \mathbf{b}$ .

The error vector  $\mathbf{e}$  introduces noise into the system, which complicates the recovery of  $\mathbf{s}$ .

Although LWE gives a good deal of protection it is not very efficient to work with. Due to the size of the matrices and vector involved the key size is big and the overall computation is slower. These inefficiencies mean that LWE is not so useful for



some practical applications, for which high degree of throughput and small size of the data are needed.

LWE has been incorporated in the development of diverse cryptographic constructs which include public key encryption, key exchange, and the digital signature. In spite of its inefficiencies, LWE is widely used in constructing cryptosystems owing to its simplicity and rigorous signals.

### **Shortest Vector Problem and Closest Vector Problem:**

Lattice problems play a central role in computer science and particularly in cryptography. These problems are based on mathematical structures such as lattices and are important to cryptographic systems due to the difficulty of solving them. What makes lattice based cryptosystems particularly important is that some of these problems are known to be secure even from quantum computers, which can be a defensive for the future cryptography.

Lattices can be thought of as grids formed by vectors, and when we study them, we're often concerned with two key problems: two of these are the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). Such difficulties arise within the context of optimization over lattice structures. Namely, in SVP, the goal is to determine the lattice's shortest non-zero vector according to a given norm with a common norm being the Euclidean norm, which is like measuring distance in the same way as distances separating two points in space. In cryptosystem terms, what is usually considered is an approximation to SVP, where one wants to find a vector that is at most a factor of  $\gamma$  away from the shortest vector in the lattice.

### **Shortest Vector Problem (SVP):**

SVP challenges you to identify the shortest vector in a lattice. Essentially, given some basis vectors – these determine the structure of the lattice and some norm such as rounding to the nearest integer, the problem is to find the shortest non-zero vector. Symbolically, this vector is defined by  $\lambda(L)$  which is the minimum length of a non zero vector in the lattice.

There exists an approximation version where instead of approximate the shortest vector one approximately the all vectors, propove with a factor at most  $\gamma \times \lambda(L)$ , where  $\gamma \geq 1$ . The hardness of SVP has tremendously important applications in cryptography despite the fact that approximating it is very hard even though there are easier approximations.

### **Closest Vector Problem:**

SVP is a generalization of CVP. Unlike before where a lattice contains all possible vectors with integer coordinates and we are supposed to find the shortest vector in the lattice, here we are supposed to given a target vector which may or may not be in the lattice, find the vector nearest to the target vector in the lattice. This is more challenging because the target vector is not necessarily in the lattice.

What's more, there is the approximation version of CVP where the goal is to find a vector that fall within the proximity of  $\gamma$  times the distance to the closest vector.

There is a close relationship between SVP and CVP in cost management for business and its strategic planning.

It was illustrated that SVP can actually be considered as the same as CVP and, therefore, solving CVP, one is also capable of addressing SVP. However, if one is to directly use the CVP algorithm to solve the problem of finding the shortest vector, it will not yield the correct result as the vector 0 is always present in the lattice. In order to avoid that, there are specific transformation which are applied to the problem and make the problem solvable.

#### **Hardness of CVP:**

Like SVP, CVP is also difficult to solve. To this extend, several researchers have established that if SVP is hard, then so is CVP. Furthermore, even obtaining an approximate optimal solution for CVP within a factor is also NP-hard which implies that it cannot be solved easily for large inputs unless some basic assumptions of computation theory are false.

Shortest Vector Problem and Closest Vector Problem:y, one can say that SVP and CVP are two of the prototypical problems in lattice-based cryptography. Because of the above reasons, the above problems are difficult to solve, and hence make cryptographic schemes based on these problems secure, especially in an environment, where we expect quantum computers to break most of the conventional cryptographic systems.

#### **Ring Learning with Errors (RLWE):**

RLWE or Ring-Learning With Errors is an algebraic variant of LWE but it is efficient because of the use of **polynomial rings**. While the operations in the RLWE are performed over general vectors and matrices like an ordinary linear space, it uses elements of a ring, particularly a ring of polynomials in most of the cases which makes the operations more optimizing.

The RLWE problem can be expressed as:

- Given a polynomial ring  $\mathbb{Z}[x]/(f(x))$ , where  $f(x)$  is typically a cyclotomic polynomial.
- The goal is to recover a secret polynomial  $s(x)$  from an equation of the form

$$a(x) \cdot s(x) + e(x) = b(x) \pmod{f(x)},$$

where  $e(x)$  is the error polynomial, and  $a(x)$  is a random polynomial. The above computations reveal that working in ring is more structured than doing computation in the complex field hence RLWE based cryptosystems is favored by the inherent cyclic nature of the ring.

RLWE is shown to offer major efficiency enhancements over LWE by operating under the framework of an algebraic structure. It has been observed that polynomial rings result to fast computations as well as small keys which are important for the formation of concrete cryptographic systems. This makes RLWE more desirable for applications where system efficiency in terms of performance and resources is paramount.

Like LWE, the security of RLWE is proved on the basis of difficult lattice problems. However, RLWE specifically capitalises on the hardness of the problem that arises in context of ideal lattices, which are in turn structured lattices that correspond to ideals in ring. RLWE keeps the characteristics of LWE resistance against the quantum threat, and therefore is equally effective in the post-quantum setting.

In particular, RLWE has been applied in various applications in practical cryptosystems including homomorphic encryption post-quantum encryption schemes. HElib and Kyber post-quantum cryptosystems employed the RLWE in their operations to enhance on their efficiency and security. Due to the efficiency in the operations of RLWE, the algorithm has been employed as the foundation of several complicated cryptographic protocols.

**Rings of Polynomial:** A ring of polynomials is an algebraic structure where polynomials have coefficients from a ring  $R$  and a variable  $x$ . A polynomial  $f(x)$  is expressed as:  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

where the coefficients  $a_i$  are from  $R$ , and  $n$  is the degree of the polynomial (the highest power of  $x$  with a non-zero coefficient).

**Module Learning with Error (MLWE):**

Module-Learning With Errors (MLWE) generalizes both LWE and RLWE by introducing **module lattices**. Modules are algebraic structures that can be thought of as vector spaces over rings, allowing MLWE to combine the flexibility of LWE with the efficiency of RLWE. MLWE essentially allows the cryptographic scheme to operate over modules instead of just vectors or rings, creating a middle ground between the two.

**Module lattices** are a class of lattice structures that arise from the algebraic setting of modules over rings. They generalize the concept of traditional lattices by incorporating additional algebraic structure from modules, which are similar to vector spaces but with scalars coming from a ring instead of a field.

The MLWE problem can be described as:

- Given a matrix  $\mathbf{A}$  over a ring, a secret module element  $\mathbf{s}$ , and an error vector  $\mathbf{e}$ .
- The goal is to recover  $\mathbf{s}$  from the equation  $\mathbf{As} + \mathbf{e} = \mathbf{b}$ .

MLWE strikes a balance between the generality of LWE and the efficiency of RLWE. By operating over modules, MLWE enables more flexible cryptographic schemes

with smaller key sizes and faster computations than LWE, while still maintaining more generality than RLWE. MLWE has become a preferred choice for cryptosystems that require compactness and performance without sacrificing security.

MLWE retains the security guarantees of both LWE and RLWE by reducing to **module lattice problems**. These problems are just as hard as general lattice problems, ensuring quantum resistance. The additional structure of modules allows MLWE-based cryptosystems to be more flexible while maintaining robust security.

MLWE has found its use in cryptographic protocols where efficiency and flexibility are both critical, such as **public-key encryption schemes** and **key exchange protocols**. By providing a middle ground between LWE and RLWE, MLWE offers the best of both worlds—efficiency for practical deployment and flexibility for various cryptographic needs.

## 3.2 Public Key Encryption, Post-Quantum Cryptography, and Kyber

### 3.2.1 Introduction

In the modern world where communication can occur over insecure networks, secure communication is vital. PKE has been extremely useful when it comes to data security that is involved in the transmission of data over the internet. But the risk of quantum computing threatens the present cryptographic systems, and so gives rise to the Post-Quantum Cryptography (PQC). One of the most prospective PQCs is a CRYSTALS-Kyber which is a quantum-safe KEM chosen by the US NIST for standardization.

#### The Current Challenge

Modern communication protocols rely on asymmetric encryption, which uses Key pairs. The Diffie-Hellman key exchange protocol, for example, allows two parties to establish a shared secret key without prior secure communication.

#### Key Generation and Exchange:

Each party can create a secret key and as a result develop the other counterpart key known as the public key. In this process, they transfer their public keys through an insecure channel.

#### Shared Secret Derivation:

Here both parties apply one's private key and the other party's public key in order to arrive at the same secret key. The security of Diffie-Hellman is based on the discrete logarithm problem which is intractable for classical computers, but can be solved by using Quantum computers and more specifically, Shor's algorithm making current cryptographic systems vulnerable [39].

| Feature      | LWE   | RLWE   | MLWE  |
|--------------|---|--|---|
| Structure    | Vectors over finite fields                        | Polynomials over rings                                 | Modules (vector spaces over rings)            |
| Problem      | Matrix-vector multiplication with error           | Ring multiplication with error                         | Matrix-module multiplication with error       |
| Efficiency   | Least efficient, larger keys                      | More efficient due to ring structure                   | Balance between LWE and RLWE, efficient       |
| Key Size     | Large   | Smaller due to ring structure                          | Smaller than LWE, larger than RLWE            |
| Security     | Based on general lattice problems                 | Based on ideal lattice problems                        | Based on module lattice problems              |
| Applications | Post-quantum encryption, signatures, key exchange | Homomorphic encryption, efficient post-quantum schemes | Public-key encryption, post-quantum protocols |

**Table 3.1.** LWE vs RLWE vs MLWE: A Comparison

## **The Solution: Post Quantum Cryptography**

Post-Quantum Cryptography (PQC) aims at constructing a cryptosystem which is resistant to both classical and quantum attacks. PQC is useful when addressing problems that are difficult for both classical and quantum computers, and this promotes the stability of cryptographic procedures in the future world with more quantum computers.

### **PKE to KEM Key Encapsulation Method**

Public Key Encryption (PKE): In this technique, a message is encrypted with the help of a key called the recipient's public key and generate a ciphertext that can only be decrypted by the recipient's private key.

Key Encapsulation Method (KEM): KEM involves securely transmitting a pre-determined shared key using asymmetric encryption: KEM involves securely transmitting a pre-determined shared key using asymmetric encryption. The sender then also comes up with what is called a secret key and proceeds to encrypt the message with the recipient's public key thus creating the ciphertext. The recipient then uses his/her private key to decrypt the ciphertext in order to obtain the shared key. Then this shared key is used for the operation of actual communication data through the method of symmetric encryption.

The primary difference between PKE and KEM lies in their methodologies: PKE is for encrypting any message of the sender's choice while KEM is used to securely passing a key which has already been agreed on.

This was after in 2022 where NIST chose CRYSTALS-Kyber for post quantum cryptography standardization. CRYSTALS, which stands for Cryptographic Suite for Algebraic Lattices, includes two components: CRYSTALS, which stands for Cryptographic Suite for Algebraic Lattices, includes two components:

- Kyber: a key encapsulation mechanism (KEM).
- Dilithium: A digital signature algorithm .

Kyber is developed to offer quantum-safe security using lattice-based cryptography. Kyber provides another public-key encryption that sets up symmetric keys for further high-level protocols including TLS and OpenPGP. Depending on the hardness of the Module-Learning-With-Errors (MLWE) problem, it works on polynomial rings and is quantum secure.

| Version   | Security Level | Private Key Size | Public Key Size | Ciphertext Size |
|-----------|----------------|------------------|-----------------|-----------------|
| Kyber512  | AES128         | 1632             | 800             | 768             |
| Kyber768  | AES192         | 2400             | 1184            | 1088            |
| Kyber1024 | AES256         | 3168             | 1568            | 1568            |
| RSA3072   | AES128         | 384              | 384             | 384             |
| RSA15360  | AES256         | 1920             | 1920            | 1920            |

**Table 3.2.** Kyber Security Levels

### The Key parameter and the Different levels of Security

Kyber is defined with three security levels, each balancing key size and security.

## 3.3 Kyber by Example

To further understand Kyber, consider a more basic variant known as Baby Kyber, which retains the essential concepts of Kyber but with less requirements.

[40]Here's a more detailed explanation of the key generation process in Baby Kyber: We are taking  $q = 17$  and the polynomial modulus we'll use is  $f=x^4+1$

1. **Private Key Generation:** The private key  $s$  is represented as a vector of two polynomials,  $s_1(x)$  and  $s_2(x)$ , each having small integer coefficients. For example, the private key could be:

$$s = (-x^3 - x^2 + x, -x^3 - x)$$

These polynomials are randomly generated with small integer coefficients, often within a small range (e.g., from -1 to 1 or another small range depending on the parameter set).

2. **Public Key Generation:** The public key in Baby Kyber consists of two main components: a matrix of random polynomials  $A$  and a vector of polynomials  $t$ .
3. The matrix  $A$  is created by generating polynomials with random coefficients. These coefficients are then reduced modulo  $q$ , where  $q$  is a predefined modulus (often a prime number).
4. The vector  $t$  is computed using the formula:

$$t = A \cdot s + e$$

Here,  $A$  is the matrix of random polynomials,  $s$  is the private key vector, and  $e$  is an error vector consisting of small polynomials (similar to the polynomials in the private key). The addition of  $e$  introduces some noise to ensure the security of the scheme.

In our example : we will have A as

$$A = \begin{pmatrix} 6x^3 + 16x^2 + 16x + 11 & 9x^3 + 4x^2 + 6x + 3 \\ 5x^3 + 3x^2 + 10x + 1 & 6x^3 + x^2 + 9x + 15 \end{pmatrix}$$

and t would be  $t = (16x^3 + 15x^2 + 7, 10x^3 + 12x^2 + 11x + 6)$ .

In summary:

- The private key is a vector of two small polynomials.
- The public key consists of the matrix A (with random coefficients reduced modulo q) and the vector t, which is computed as

$$t = A \cdot s + e$$

### 3.3.1 Encryption Process

#### Random Polynomials:

For each encryption, a randomizer polynomial vector r and error vectors e1 and e2 are generated. These are small polynomials with coefficients that are typically within a small range (e.g., -1, 0, 1). Example:

$$r = (-x^3 + x^2, x^3 + x^2 - 1)$$

$$e1 = (x^2 + x, x^2)$$

$$e2 = -x^3 - x^2$$

#### Message Encoding:

The message, represented as a binary number, is converted into a polynomial. For instance, the number 11 (binary 1011) is encoded as:  $m_b = x^3 + x + 1$  This polynomial is scaled by multiplying it with  $\lfloor \frac{q}{2} \rfloor$ .

With q=17, this scaling factor is 9:  $m = 9 \cdot m_b$   $m = 9x^3 + 9x + 9$

#### Ciphertext Computation:

The public key (A,t) is used to compute two components u and v  $u = A^T \cdot r + e_1$   
 $v = t^T \cdot r + e_2 + m$

Example ciphertext:  $u = (11x^3 + 11x^2 + 10x + 3, 4x^3 + 4x^2 + 13x + 11)$   $v = 7x^3 + 6x^2 + 8x + 15$

The ciphertext is the pair (u,v).



### 3.3.2 Decryption Process

#### 1. Message Recovery:

The recipient uses the private key  $s$  to compute a noisy version of the message

$$m_n$$

$$: m_n = v - s^T \cdot u \text{ Example: } m_n = 7x^3 + 14x^2 + 7x + 5$$

#### 2. Message Rounding and Recovery:

Each coefficient in

$$m_n$$

is rounded to recover the original message. Coefficients closer to

$$\left\lfloor \frac{q}{2} \right\rfloor = 9$$

represent binary 1s, and those closer to 0 represent binary 0s. For example, rounding the coefficients of  $m_n$  gives the binary polynomial:  $m_b = x^3 + x + 1$ . This corresponds to the original binary message 1011, or the number 11.

This process demonstrates how Kyber achieves secure public-key encryption by using structured lattice-based problems, making it resistant to quantum attacks. Careful selection of parameter sets  $(n, q, k)$  ensure that Kyber maintains a good balance between security, efficiency, and performance, making it suitable for a variety of cryptographic applications.

## 3.4 Feature Extraction and Generation of Cancelable Biometric Template

### 3.4.1 Use of Physiological Patient Data

A recent trend in research has been to encrypt data using physiological signals or generate encryption keys [41]. The physiological data is good choice for use as cryptographic keys if physiological parameters satisfy some requirements [2][19]. It should be universal, have uniqueness and time variance.

**Universality:**The physiological parameter must be measurable and obtainable from every user of the system. In other words, every person in the network must be able to provide this bio-metric trait without exception.

**Uniformity:**The physiological parameter must be different for different users at any given time. This means the biometric trait can't be easily replicated or matched between users. It prevents cross-user interference, so data encrypted with one person's physiological trait cannot be decrypted by another person's trait. This is crucial for security and privacy, so unauthorized access to secured data can't happen.

**Time Variance:** The physiological parameter should change over time for the same user. But it should remain consistent during simultaneous captures so keys can be regenerated when needed. Temporal variation facilitates key renewal. By changing over time, the physiological trait prevents long term use of a single key, which increases security by reducing the risk of key compromise.

Following points generally describe how we can use Patient's physiological data.

1. Record Physiological Information: Physiological data such as fingerprints [42], iris patterns, facial features, or heart rate are recorded using a sensor device that should be reliable and trustworthy. The physiological data possess the same property as PUF as it is inherently unique and is also difficult to clone.
2. Extracting Features and Creating Templates: Data Processing: To identify distinctive traits, process the physiological data that were collected. Generate a biometric template using these attributes [43][44].
3. Challenge Response Process: As challenges, physiological data or derived attributes can be used. Create responses by combining a cryptography procedure with the physiological data.

Heart Rate Variability is the difference in time between heartbeats. It is the analysis of heart rate fluctuations from beat to beat. The physiological parameter HRV satisfies the following requirements to be utilized as an encryption key: (i) it is globally measurable; (ii) it is individual-specific; (iii) it is chaotic in nature; (iv) it exhibits bounded

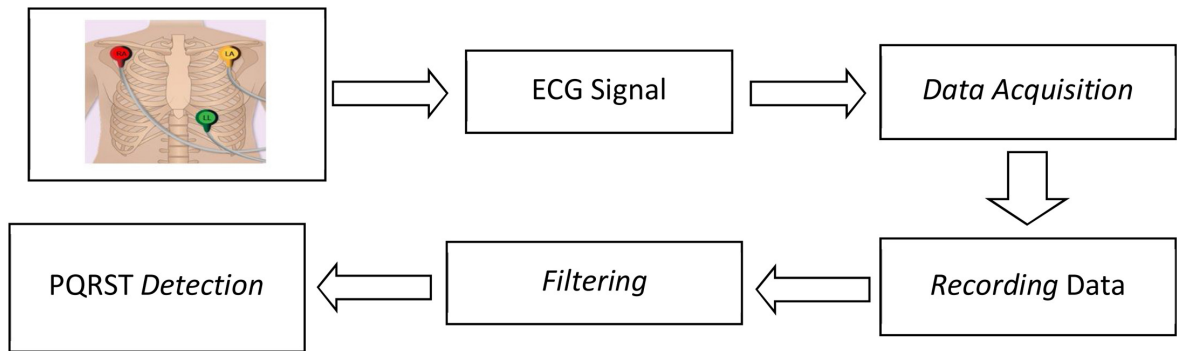


Figure 3.1: Feature Extraction from ECG

random process behavior. In terms of physiology, HRV is readily accessible through a variety of biological signals, including BP, PPG, and ECG. [45]

As we are using ECG, features like heart rate variability and QRS would be extracted [46]. EKG or ECG was invented in early 1902 by Willem Einthoven. It records electrical activity of the heart and thus displays a record that represents electrical activity of the heart. The heart has four cavities, that is two auricular or receiving chambers that collect blood and pump it into two ventricular or pumping chambers which circulate blood all over the body with oxygen adjuncts. They are movements in the electrical system that result in heart contractions and registered and read from the ECG. ECG is perhaps the most popular signal in healthcare; therefore, it covers the necessary heart function and patient's general condition.

The figure 3.1 shows the flow of data collection and feature extraction.

#### **Feature Extraction of ECG Signals:**

In ECG signal analysis, the features which are significant are identified and can be used for evaluation of the electrical function of the heart. The first components assessed are the QRS complex, P wave and T wave all of which reflect different stages in the functional capacities of a heart.

The QRS complex is composed of three waves: These are Q wave, R wave and S wave. This complex represents the ventricular depolarisation, the stage of electrical activity which makes the heart ventricles to contract. In one's ECG signal, it is the most distinguishable structure, given the high amplitude of the phenomenon. The QRS complex is unique in that it helps in finding the heart rate, and the presence and type of arrhythmias, as well as other diseases such as ventricular hypertrophy, bundle branch blocks and conduction delay. Alterations in its shape may mirror life threatening pathology such as myocardial infarction or other cardiovascular diseases.

P wave reflecting atrial activity is atrial depolarization which in physiological terms translates to the electrical stimulus that causes atrial contraction. This feature is important in diagnosis of atrial arrhythmias such as atrial fibrillation, or atrial flutter among other arrhythmias. This view also gives information about the size and

work of the atria. Pathological changes in the P wave indicate probabilities of atrial enlargement or problem with the AV node.

What is exactly seen in the T wave involves ventricular repolarization which is the process whereby the ventricles restore their electrical status for contraction. Abnormalities in the T-wave can be signs of myocardial ischemia, disorders in electrolyte balance or the effects from a medication. The T waves are also utilized to evaluate the possibility of a cardiac event occurring in future due to appearing in an abnormal manner.

Apart from these ideal features, several other intervals and segments are of cardinal importance in the study of the cardiac rate and rhythm. The PR interval is the time period from the start of the P wave to the start of the QRS complex, which represents the time taken for electrical conduction between the atria and ventricles. Any kind of abnormality in PR interval may be attributed to some kinds of heart block or pre-excitation syndromes. The QT interval which is the time between the start of the QRS complex to the end of the T wave, measures total time required for ventricular depolarization and repolarization. QT interval of the ECG is an indicator of refractory period and normally lasts between 0.44 seconds and 0.50 seconds; however, prolonged or shortened QT intervals have been linked with arrhythmias and may be caused by genetics or medications or electrolyte imbalances. Finally, the ST segment, the horizontal line between the end of QRS complex and the beginning of T wave is important and should be different from the usual baseline if it is to depict myocardial ischemia or infarction.

In conclusion, these components of physical configuration of an ECG signal, namely QRS complex, P wave, T wave, and other intervals and segments mentioned above, are the basic requirements for assessing the state of a heart [47]. They offer important information about the state of the heart and help to determine various disorders, estimate the heart rate, reveal needed rhythms, and evaluate the treatment result. To have proper diagnosis and management of the heart, there is need to have good interpretation of these features.

**Use of ECG in Cryptosystem:** The incorporation of ECG into cryptosystems is a relatively new category of employing uniqueness in biometric data for better security. Thus, ECG signals which represent the electrical signals generated by the heart can be used for biometric authentication because they vary significantly from person to person. The shape, the amplitude, and the timing of the ECG waveform differ from one person to another making it a biometric type of the person just like fingerprints or iris scanning. From these unique characteristics it is quite straightforward to identify the user through his or her specific heart pattern, which makes the cryptosystems ideal for identity authentication.

Besides biometric authentication, it is possible to use ECG signals for cryptographic key generation. Because an individual's ECG signal has several factors that are peculiar to him or her in making a signature, it can be turned to a secure key that

is very difficult for other people to imitate. It can then be used in any cryptographic method to secure information and connections. This characteristic of ECG data means that the created key is likely unique to the person and difficult for another individual to replicate, further strengthening the existing cryptographic system.

Another benefit of using ECG signals is that it can provide users with continuous authentication. ECG-based systems can allow for repeated authentication within a session, unlike other methods that only offer a single check. Since the ECG signal captures the heart activity in real-time, this ensures constant authentication of the user, thus reducing instances of mimicry or impersonation to gain access to some critical systems, which in turn increases security.

Furthermore, with the permission of the user, the ECG data can also be incorporated into different layers of identification and used as an additional measure in the identification process. By integrating ECG signals with other means of authentication, for instance, passwords, fingerprints, ECG signals offer additional layers of security that make it challenging for the attacker to penetrate the system. This layers of security make it very reasonable since security is never overemphasized to be a product of one method alone.

Including ECG features for key generation in the biometric cryptographic system is unique in developing the cryptographic key for individual usage. This method builds up the employment of physiological signals such as electrocardiogram of human to improve security in cryptographic applications due to the physiological signals physiological signals are unique in both their acquisition and their dynamic variability in time.

**Uniqueness and Variability** It is characteristic that QRS complex, P wave and T wave of the ECG signal reveals separate and clearly distinguishable pattern for every person. These features include the times, frequencies, and general forms of the waves and are ideal for development of user-specific cryptographic key. Furthermore, ECG signals are intrinsically non-stationary, and thus the temporal variability also fortifies the security paradigm. Such temporal variability guarantees the generated keys not only to be diverse but also to follow the natural fluctuations in ECG signal.

### **Steps for Key Generation**

The first step is to extract necessary features of the ECG signal that is to be analyzed. These consist of R-R intervals, amplitude ratios and wave durations— where R-R intervals refer to the time intervals between successive R-peaks in the QRS complex; the amplitude ratios include the ratio of the amplitude of the P wave, the amplitude of the QRS complex, and the amplitude of the T wave; and the wave durations include the time durations of the P wave, the QRS complex and the T wave. These features hold the nature of ECG signal and are the basis of seven features which are related to the key generation [48] [49][50].

After the features have been determined, they are transformed to digital formats that can be used for cryptographic purposes. This quantization process converts the

ECG signals to discrete form from a continuous form, for example; binary or integer from, is suitable for incorporation in cryptographic algorithms. Key Derivation: The quantized features are then summed up in order to obtain a cryptographic key. This process may require hashing of the features or applying other operations like XOR or by using fuzzy extractors. This paper also demonstrates how fuzzy extractors are invaluable for dealing with inevitable fluctuations in the ECG signal so that the derived key is both secure as well as reproducible from similar ECG data.

The derived key is the key that is then utilized in performing a cryptographic operation of either encryption, decryption, or even authentication. Rather than storing the key the key is derived out from the ECG signal each time it is required, thus making it current and secure.

### **Applications:**

**Healthcare Security:** Keys generated from ECG can be applied for protecting patients records or medical devices and interfaces in order to prevent unauthorized access to patients' personal details.

**Continuous Authentication:** In this way, by periodically comparing the new portion of the ECG signal the system can restore the key and deliver the authorization continuously. This method also increases security since access is limited to the said authorized individual throughout the session.

**Biometric Encryption:** The various keys as derived from the ECG signal of a patient can be used to encrypt other personal health data such as the digital health record thus making personal health data more secure.

Altogether, integration of ECG features for the key generation in the cryptographic systems is secure and personalized for the encryption and authentication. The method builds on the features of the ECG signals being unique yet random, making it improve the security of the cryptographic operations and solve major problems associated with reproducibility, non-invertibility, and privacy.

To make the detection of R peaks in ECG signals richer, a number of approaches have been used. Some of them are the Derivative method, Hamilton–Tompkins algorithm, Pan-Tompkins++, Wavelet transform and Hilbert transform (HT) method. All the three methods listed above have their own advantages when it comes to identifying R peak in the ECG waveform. They also require certain factors to be investigated when comparing Hamilton–Tompkins algorithm, wavelet transform, the HT method, and Pan-Tompkins ++ with their applicability to ECG signal R-peak detection for generating cryptographic key as follows; Real-time capability , noise-rejecting capability, computational complexity and efficiency and their accuracy.

The Hamilton–Tompkins algorithm is characterized by high real-time processing capabilities and significantly faster QRS complex recognition in relatively low interferences ECG signals. Nevertheless, it is sensitive to noise that negatively influences the accuracy of detected R-peak and, as a result, the quality of keys derived from these signals.

The wavelet transform provides a high accuracy at the same time high robustness to noise; which makes the method suitable for detection of R-peaks in clean as well as noisy ECG signals. It gets information both on time scale and frequency scale so gives detailed information on various scales. In fact, although the wavelet transform is highly accurate, it is a heavy process in terms of computations which makes it inefficient for real-time processing especially in conditions where resources are tight.

The Hilbert transform (HT) method generates an analytic signal from the ECG and allows to compute the instantaneous amplitude and phase. This method is also capable of detected R-peaks with reasonable precision while as stated above the algorithm is sensitive to noise and since it is less commonly used in this context the use of this method for key generation could be unreliable.

The most common method of identifying the QRS complex in ECG signals is through the use of Pan-Tompkin algorithm. In the Pan-Tompkins algorithm, some changes are made and given a name Pan-Tompkins++ by [51] to increase the noise resistance and decrease the false alarms number. The given model gives a reasonable accuracy to noise ratio and computational complexity necessary for real-time applications. This algorithm is especially useful in cryptography key generation to be used in real-time applications since this requires high accuracy.

**[51] algorithm Pan tompkin ++ Key improvements include:**

Enhanced Filtering: To overcome these problems the author proposed the filter combination of a bandpass filter with a passband of 5-18 Hz and an N-point moving average filters.

Adaptive Thresholding: A second, more sensitive, initiating threshold that reaches the first threshold every 10ms, and a third constant, returning threshold that estimates the R-peak with higher precision in case there are processing noises or considerable signal morphological alterations.

Reduced False Positives/Negatives: The algorithm further minimizes false positive and negative rates than the simple ones by the following rules in threshold adjustment and peak classification.

Improved Execution Time: It should also be noted that, along with the increase in the efficiency of detection and accurate definition of the object's location, the proposed algorithm is also characterized by a shorter execution time in comparison with the same algorithm with classical optimization, which is approximately 33%.

Due to requirement of the wearable sensors being lightweight, use of puf for the device authentication adds the computing burden associated with creating and utilizing PUF-based cryptographic keys could impact the device's performance, possibly causing other features to lag or demanding the use of more powerful CPUs. This framework simultaneously provides quantum-safe storage and transmission of data, while giving patient control over its data and mitigating insider threat in Cloud KMS.

Following Table 3.3 provides comparison

| Algorithm         | Real-Time Capability | Noise Robustness | Computational Efficiency | Accuracy in R-Peak Detection | Suitability for Key Generation |
|-------------------|----------------------|------------------|--------------------------|------------------------------|--------------------------------|
| Hamilton-Tompkins | High                 | Moderate         | High                     | Moderate                     | Moderate                       |
| Wavelet Transform | Low                  | High             | Low                      | High                         | High                           |
| Hilbert Transform | Moderate             | Low              | Moderate                 | Moderate                     | Low                            |
| Pan-Tompkins++    | High                 | High             | Moderate                 | High                         | High                           |

**Table 3.3.** Feature Extraction Algorithm Comparison

A “cancelable template” as a security-layer aimed at improving privacy and protection of biometric data, including fingerprints, faces, or any ECG signals. The concept addresses a significant challenge: biometric characteristics are very personal and permanent by nature and therefore, if exposed, can be abused. Different from PINs or passwords that can be altered, biometric data do not change and therefore need enhanced security measures.

The concept behind cancelable template is to operate on the original biometric data with some transformation applying a function which is impossible to reverse. It implies that the original biometric data cannot be retrieved from the transformed biometric data once they undergo the transformation process. For example, when the ECG features are transformed into another form using a transformation process, even if the transformed template is disclosed, the original ECG data will not be leaked out. As this is a non-invertible transformation, original biometric data is safe from unauthorized access or reconstruction.

In addition to non-cancelable tags, an important aspect of the cancelable template is that the applied transformation is tied to the user and can be replicated. This means that each user is assigned a unique transformed template even though there may be several users with the same biometric feature. However, the transformation has to be idempotent: that is, when the same user inputs their biometric data again, the system delivers the same transformation. This is important especially when matching has to recur during an authentication or identification process.

When it comes to security, cancelable templates offer numerous advantages. This way, the users’ privacy is protected better since the original biometric data cannot be derived from the transformed template. Also, if a cancelable template is hacked, it can be ‘cancelled’, meaning that a new transformation can be adopted meaning that the actual biometric data is safe. It also helps in reducing the vulnerability of biometric data to hacker attacks and other abuses, which further improves the general stability



of biometric systems. So we are Extracting feature and making cancelable template to protect the privacy of the feature extracted.

### **Shimmer Wearable Sensor and Data Set:**

For keys derivation from physiological data, we are using data set from shimmer sensor. The Shimmer wearable sensor is a sophisticated tool developed for the recording of various physiological parameters such as ECG. Due to its accuracy and flexibility, The Shimmer sensor is employed widely in both research as well as clinical measurement because it provides full-resolution data in a tiny, wearable package. Some of this device's advantages includes; The ability to collect data with high accuracy, Comfortable to wear and its ability to support other sensors such as accelerometers and gyroscopes. Also, it offers wireless communication, whereby it is possible to transfer data in real-time to other connected devices or preserve data on the cloud for other analytical procedures.

The ECG dataset offered by Shimmer can be considered as benefit for multiple purposes. From this data, researchers are able to adapt and improve source codes for assessment of heart rate variability, diagnosis of arrhythmia and other cardiac dysfunctions. The same data set is used for assessment of ECG analysis algorithms in conditions close to real life and is widely used in teaching material to explain the nature of the ECG signal and the principles of the ECG signal analysis.

Shimmer ECG dataset is high sampling rate usually at 250Hz or 500 Hz which is quite beneficial to capture the cardiac signals in a better and more efficient manner. The data quality is preserved with clean signals which are well annotated and usually delivered in CSV. The users should go to Shimmer Support Sample Data, choose ECG sample data and download the files from the given links. Additional information regarding the formats of the data collected, the rates of sampling and other related information can be retrieved from the documentations that are provided.

Some of the possible applications of Shimmer ECG dataset include designing and validating algorithms for heart rate variability and arrhythmia analysis, using the dataset as training set for machine learning algorithms for ECG classification, and as demonstration of ECG signal analysis.

The Data Set contains the following columns:

**Timestamp:** The time at which each ECG reading was recorded.

**ECG LARA mV:** The voltage measured between the left arm and right arm.

**ECG LL RA mV:** The voltage measured between the left leg and right arm.

**ECG RESP mV:** Respiratory data in millivolts.

**ECG Vx RL mV:** The voltage measured between an unspecified point (Vx) and the right leg.

The ADS1292R is a low power, multi-channel analog front-end (AFE) that is optimized for high-resolution electrocardiogram (ECG) and respiration. This device

|               |  |
|---------------|--|
| Source        | ADS1292R                                   |
| Channels      | 4 Channels (LA-RA, LL-RA, LL-LA and Vx-RL) |
| Sampling Rate | 1024 Hz                                    |
| Format        | 24 bits, signed                            |
| Units         | mV   |
| Filtering     | None                                       |

**Table 3.4.** ECG data source and its characteristics:

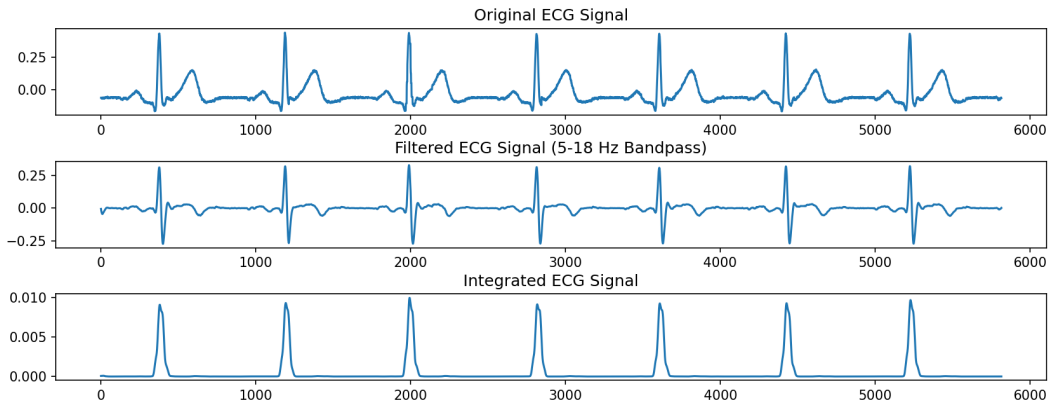


Figure 3.2: Filtered ECG Signals

has four input channels, namely: LA-RA, LL-RA, LL-LA, and Vx-RL which record unique aspects of the bio-potential signals. LA-RA is useful for recording heart signals and measures the voltage between the left and right arms; LL-RA is another channel that records the voltage between the left leg and right arm, which is analytical for heart electrical charges; LL-LA records voltage between the left leg and left arm and is another component of ECG; and Vx-RL measures an unspecified point and right leg for recording other signals including respiration. The ADS1292R works at a high sampling rate of 1024 Hz in order to capture detail in the signal and record the signal 1024 times per second. Every sample is taken at 24-bit which helps in capturing small details when it comes to electrical signals and the data is in form of Millivolts (mV) as a result of the heart activities. Critically, no filtering takes place on the raw signal and hence while it records all the electrical activity, subsequent filtering is required to eliminate undesirable signal such as muscle noise or baseline drift.

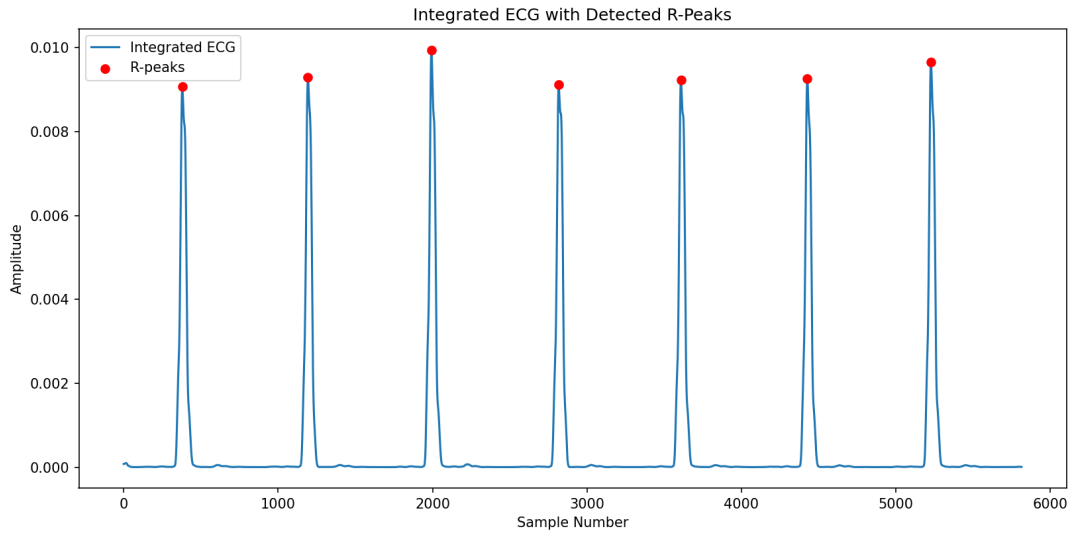


Figure 3.3: Detected R Peak

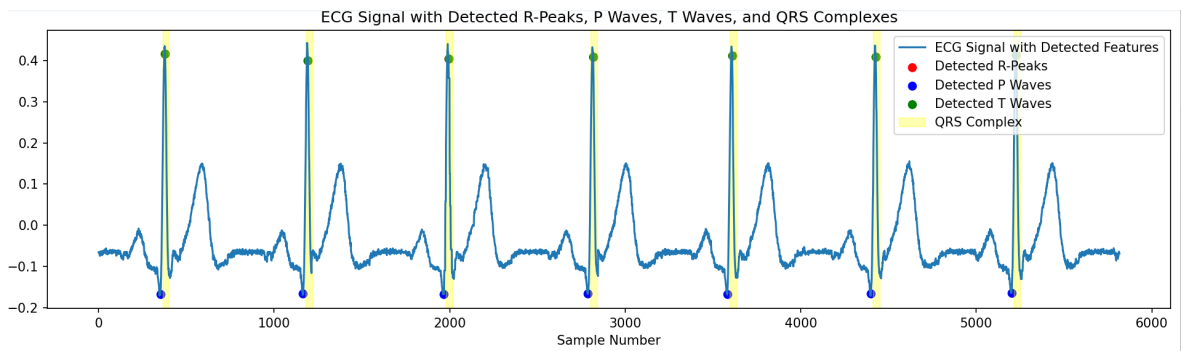


Figure 3.4: Detected Peaks

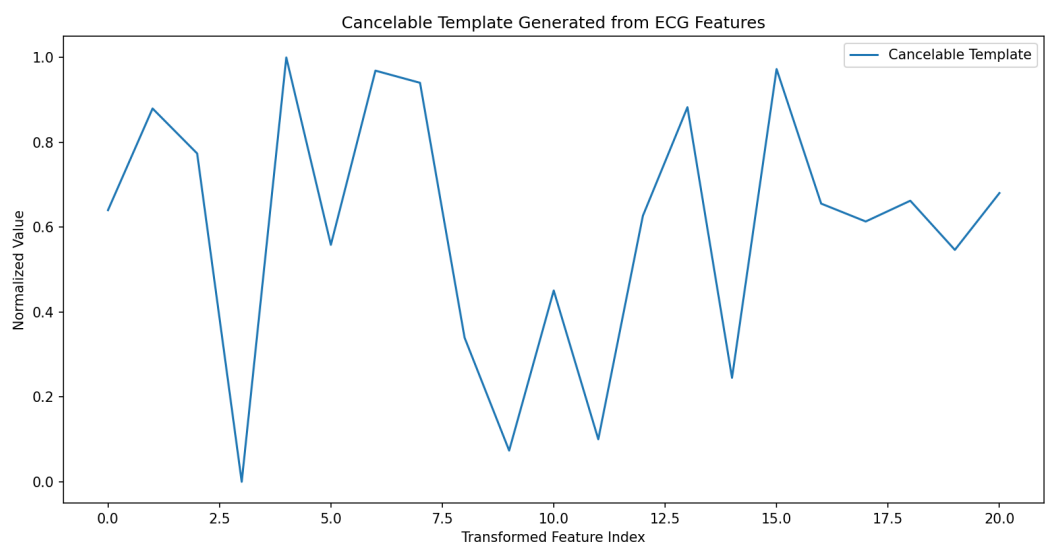


Figure 3.5: Cancelable Template Generated

# Chapter 4

## PROPOSED HOSPITAL KEY MANAGEMENT SYSTEM

### 4.1 System Component

#### 4.1.1 Patient Sensor - Wearable Device

This Sensor device collects a patient's health information and encrypt it using a key that is generated from Master key. The master Key is locally generated and stored in the device. This Key is never itself shared directly, but is used to derive keys derived from it.

#### 4.1.2 Hospital Server

Central storage and processor for patient data. . It receives the encrypted data from the sensor, store it, decrypts data when doctor or other medical entity request it by the consent of the Patient.

### 4.2 Process Flow

The first step in the proposed model is the device registration. In the following section describe how the registration of the device will take place. It is acceptable to presume that the patient has visited the healthcare institution in person before to the start of the monitoring, as they will be a part of an application for continuous monitoring. Patient bought the sensor device for monitoring.

**Device Registration and Binding to Patient Process:** A vital step in guaranteeing the precise and safe monitoring of patient data is the registration of a patient’s sensor equipment with the hospital system. The authorized technical staff at the healthcare facility assists in this registration process in order to guarantee the process’s security and integrity. Within the medical institution, a specialized, physically secure server is used to complete the device registration process. The registration procedure is safeguarded against unauthorized access and tampering by the fact that this server is located in a controlled environment that is only accessible by authorized technical professionals.

**Identification and Assignment of Device:** During the registration procedure, each sensor device is given a unique identity, also known as the Sensor ID. This Sensor ID is necessary to link the device to the correct patient data and is used to identify the device specifically within the hospital’s network. A distinct ID is given to the patient under observation. In order to ensure that the data acquired by the sensor is accurately attributed to the appropriate patient, the Sensor ID and Patient ID are securely tied together in the registration procedure. A secure cryptographic procedure is used to bind the Sensor ID to the Patient ID. This procedure guarantees that the connection between the sensor and the patient is unadulterated and can be verify by the HS.

We are using patient physiological Data to bind sensor and the patient with each other.

1. Collecting Patient Physiological Record:

- (a) Initial Data Capture: While the patient is first being registered at the medical institution, a sample of their physiological data (such as their heart rate, ECG, PPG, etc.) is collected by their wearable sensor. Cryptographic keys can be generated using this data, which functions as a distinct bio metric signature.
- (b) Extracting Features:

To extract distinguishing traits, the sensor or a linked device processes the raw physiological data. A bio metric template, a distinct digital depiction of the physiological data, is created using these characteristics.

**ECG Signal Processing and Cancelable Template Generation:**

The first node of the process is the ECG\_Signal which is the raw signals obtained from the electrocardiogram gotten from a CSV file. This signal is sampled at a frequency of 250 Hz which is an important parameter of Sampling\_Rate. This procedure ultimately aims at creating a Cancelable\_Template. This template is obtained after passing the ECG signal through different steps such as filtering, feature extraction and transformation. The cancelable template is a

secure, transformed form of the original data for improving the privacy-level over the original data against external threats.

In analysing ECG signals, a number of steps are carried out in the preprocessing phase of the preprocessed data set. First, pre-processing of the collected ECG signal undergoes the bandpass filtering where the range of frequencies is set between 5-18 Hz to counterbalance the amount of noise present and to maintain frequencies which are more relevant to cardiac activities. Subsequently, differentiation is performed on the filtered signal which amplifies high-frequency changes especially the QRS complexes which are rapid. To make the peaks of the differentiated signal even more pronounced, each point of the resulting signal is squared, which makes the peaks even sharper. Subsequently, to remove noise, the signal is smoothed over 60ms with a rectangular window on the squared signal. Last but not the least, a moving window integration of 150ms is applied on the smoothed signal for extracting and amplifying several other important characteristics necessary for effective ECG analysis.

In the decision phase of ECG signal processing, the algorithm is concerned with the identification of the most relevant characteristic features of cardiac origin and their categorization accordingly. First of all, the peak points of the integrated ECG signal are identified, but only those that are localized at least 231 ms from each other remain in further analysis to consider the time of the heart's refractory period. Signal peaks (SPK) and noise peaks (NPK) are set and Dynamic Threshold 1 and Dynamic Threshold 2 are generated. The Threshold1 is used to classify the data points which are higher than this threshold as R-peaks and the threshold is adjusted over time depending on the detected R-peaks. When more than eight R-peaks are identified, the algorithm computes the RR interval, to distinguish between T-waves, QRS complex and R-peaks using some specified rules.

In the present algorithm for detecting P and T waves, the algorithm looks for P-waves within a window of 200 milliseconds prior to R-peak and T-waves within a window of 400 milliseconds following a R-peak.

Following the detection of these waves, it then formulates a cancelable template for the system. This involves mapping the detected R-peaks, P-waves and T-waves into a feature vector in which a randomly generated projection matrix is applied to produce the cancelable template. This change conceals the previous characteristics, and can hardly be reversed. The cancelable template is then normalised and stored in a CSV file that is beneficial for future use.

The Sensor ID and the Patient ID are cryptographically linked using the Binding Key, which is obtained from the patient's physiological data. This binding guarantees that particular sensor can only be linked to the patient who has the

corresponding physiological data. This key is used by the sensor for identification and for non repudiation in the future.

The identity of this device will be denoted as Sensor ID. The identity assigned to the patient for monitoring purposes is denoted as Patient ID.

$$ID = KDF(SensorID + PatientID + ECGFeatures) \quad (4.1)$$

We also need another high level key which serves the purpose to derives other keys. Within the wearable sensor device, the Master Key serves as the main cryptographic key. It acts as a root of trust within the device, providing the security framework for all other keys and functions. It adds an extra layer of security to protect them from unauthorized access or tampering. A high-quality Random Number Generator (RNG) is used to create the Master Key. In order to prevent predictability or attacks based on key patterns, the RNG makes sure that the key have enough entropy and very random. This key would be generated during the device initialization. After it is created, the Master Key is safely kept in the secure storage module of the wearable sensor device, which could be a Secure Element (SE) or Trusted Execution Environment (TEE). Even in the case of a device compromise, this secure storage is intended to keep the key safe from unwanted access.

As an example we generated master key by importing python library secrets and using its function `secrets.tokenbytes(32)` which generated random key of specified length. This Master key will be securely stored in TEE of sensor device and will never leave outside.

$$\text{masterkey} = \text{secrets.tokenbytes}(32) \quad (4.2)$$

## 4.3 Secure Channel Establishment between Patient Sensor device and Hospital Server and Doctor

### 4.3.1 Mutual Authentication:

Our study is primarily focused on creating a secure communication channel between the Hospital Server and the wearable sensor device worn by the patient. Once the sensor device has registered, the process of creating this secure channel begins. A sensor device sends its public key to the Hospital Server on behalf of the patient. The sensor device is the beginning entity in this process as the patient starts the monitoring session. The patient's sensor device referred as Client A in this process and the entity with which the secure connection is being established, the Hospital Server is designated as Client B.



In this case, the subject being observed is the patient or the individual whose health information is being tracked. A wearable sensor is utilized by the patient to connect with the system. The doctor is the employee in the health sector that requires the patients' records for diagnosing or treatment purposes. The role of the server of the hospital is to make sure that all the information is well stored and there is also administration of both the identity of the patient and that of the doctor.

First of all, it utilizes Kyber-based key generation, which is a post-quantum cryptographic algorithm. Kyber key pair is created by the patient device through Physiological Unclonable Function (PUFF) and the key will be unique to the patient. Likewise, both the doctor and the hospital server also create their unique Kyber key pairs through methods such as HRNGs or TPMs. These key pairs also help to facilitate, authentication among the various parties that are involved in the communication process.

In the mutual authentication process, the first step is that the patient's device initiates the connection to the hospital server and shares its public key. The server also sends its public key and a random challenge to the patient and this is followed by the validation of the results and calculation by the patient of the shared secret. There is a similar process between the doctor and the server of the hospital where both the doctor's device authenticate the server and compute a shared secret. In these transactions, the patient alone and the doctor alone create two distinct secrets with the hospital server.

After both the patient and the doctor have authenticated the other, the system permits the patient and the doctor to communicate privately with each other through the hospital server. When a doctor wants to view medical data of a specific patient, the doctor must make the request to the hospital's server and the server forwards the request to the intended patient. The patient, who owns the data, can review and control who has access since the key is created by encrypting a temporary access key with the doctor's public key. This means once a patient is assigned a certain ID number, only a doctor who enters this number can decode the data and therefore the server of the hospital can't access the information without strict permission from the patient.

This keeps the patient's data safe and can only be accessed by authorized persons when necessary. In addition, the transferred data is encrypted with the help of a key which was generated with the help of the Kyber protocol from the shared secret, which helps to enhance the quantum security of a network. Although the patient's data is stored on the hospital's server, it is encrypted and cannot be accessed or altered by any party without the patient's permission.

By Using SMA technique using Kyber, the system can offer an efficient and secure solution for the hospital environments. The authentication of the patient, the doctor, and the server enables the verification of all parties, and the patient remains in

full control of their information. Kyber’s immunity to newer quantum computational breakpoints helps keep the system secure in the future, which is why it is the best choice to protect the essential health information.

Proposed approach ensures that the patient has a deep level of security and its data is protected against attacks of quantum computers while at the same time the patient has a chance to decide who is allowed to access his/her sensitive medical data.

The following important criteria motivate careful planning of the session establishment process.

1. On-Demand Key Generation :Because the shared key can be generated instantly, there’s no need to keep it, which increases security and lowers risk.
2. Quantum-Resistant Security: Long-term security can be guaranteed by strengthening the system against prospective quantum computing attacks by integrating bio-metric-based keys with post-quantum cryptography techniques.
3. Memory Efficiency: Because sensitive keys are generated only when needed and are not kept for an extended period of time, this method reduces the memory storage overhead.

The Components are:

- PQC Kyber key exchange which is used for quantum-resistant key exchange.
- Session Key: Derived from the master key for encrypting data within each session.
- Master Key: this is stored securely within the wearable sensor, and used to encrypt pairwise symmetric keys; it resides in a secure environment on the sensor.

### 4.3.2 Session Key Generation

To create a session key, the client device and HS employ the Kyber protocol. HS sends the sensor device the public key of a Kyber public-private key pair that it was created with. Sensor device A derives a key from the master key and encapsulates it and sends it back, which HS decapsulates with its private key to obtain the session key. For reference, we denote this session key as SK. A will use the key SK to send its encrypted data to HS.

If the secure communication system is a combined classical and post quantum system, using the generated session key from a master key and encrypting with a shared secret based on Kyber offers a strong layered encryption. Kyber includes its quantum-resistant features in combination with a master key locked in the sensor device which helps to improve control.

This shared secret serves as the first line of security, which guarantees that all subsequent communications between the patient and the hospital server will be encrypted using quantum-resistant mathematical algorithms. After generating the session key, the applicant encrypts it utilizing the shared secret from the Kyber key exchange. This encryption step adds an extra layer of security, because even if the attacker intercepts the session key, he or she will also have to solve the Kyber quantum-resistant encryption to get access to the key. The encrypted session key is then sent to the hospital server (or doctor) and the latter can decrypt the key using the shared secret. Once the session key has been decrypted, the actual communication/medical data between the sensor device and the hospital server (or doctor) is encrypted/decrypted using the session key during the session. This makes sure that the data in transit is protected through encryption, with the session key generated from the master key and encrypted with the shared secret.

By using Kyber, quantum resistance is achieved and the system is safeguarded against possible quantum attacks. To ensure further independence and protect the data from key usage in subsequent communication sessions, a distinct session key is used for each session. The layered security that is used here, involving the double layer of Kyber-based shared secret and the session key derived from the sensors ensures that attackers cannot easily decode the encrypted messages or intercept them in any way.

In cryptography, a session key generally refers to a type of key that is used in a single session or transaction and is short lived. The key is generated only for that particular communication session. But still if someone have stored the session key, he/she can decrypt the content of that session. In our scenario, if the doctor stored the key, he can see the content of that session without the consent of patient. To ensure that doctor always gets the consent from patient and patient have control, we need to ensure that session key should be unusable after session ends. For this purpose, we would use ephemeral session Key. This type of session key includes contextual information(session specific information) in it. This information includes session ID and timestamp. To make it random so that corresponding party cannot guessed the key, nonce value would be added too. This contextual information will be stored at patient ends. Incorporating session specific information is to enhance security so that if key used for session key is accidentally found for that particular session, it wont posses any threat. So now we have ensure that our session key would be valid for only that specific session, it would be unique per session. For every session, a new unique and short lived session key would be generated. Also, there is no use to store this key in any storage medium. It only resides in memory for only that session.

After the session ends, as the session key is short-lived, it will be discarded. HS must initiate a fresh session with the patient in order to obtain the required decryption key if it needs to access the previously sent data. This key is for only that specific decryption task.

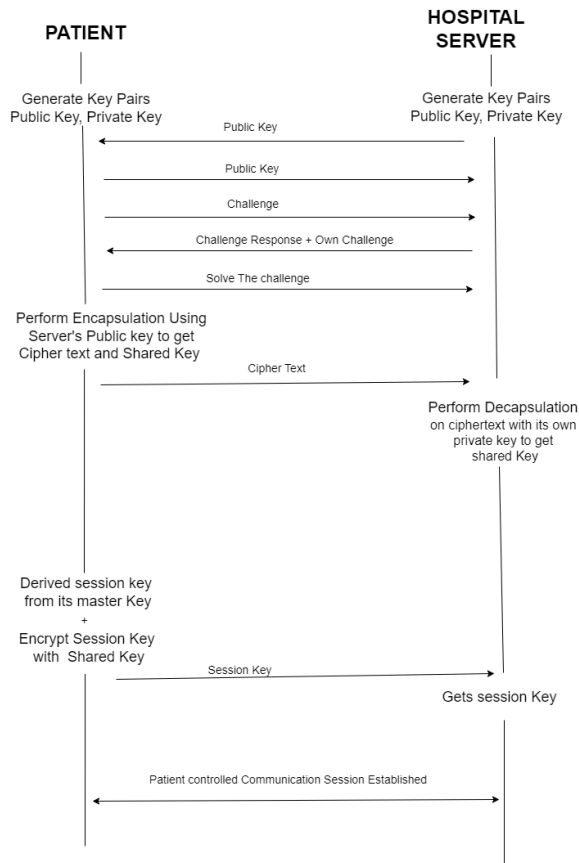


Figure 4.1: Sequence Flow Diagram

After every encryption cycle, the protocol can be used to replace out the key pairs. Because different keys will be used throughout the succeeding cycles, the possible loss of the secret keys during an encryption/decryption cycle has minimal effect.

The patient is under constant observation; it can appear that the sensor and HIS are in session all the time. But actually it refers to a particular, time-limited interaction during which a session key is used. Sessions technically "end" and "restart" as part of standard security protocols, and session keys are periodically renewed even in continuous monitoring.

Figure4.1 shows the sequence flow diagram illustrates the process flow of the proposed system.

# Chapter 5

## ALGORITHMS

This Chapter explain all the algorithms used for the implementation of our proposed system.

Figure5.1 shows the steps involve in Key generation process.

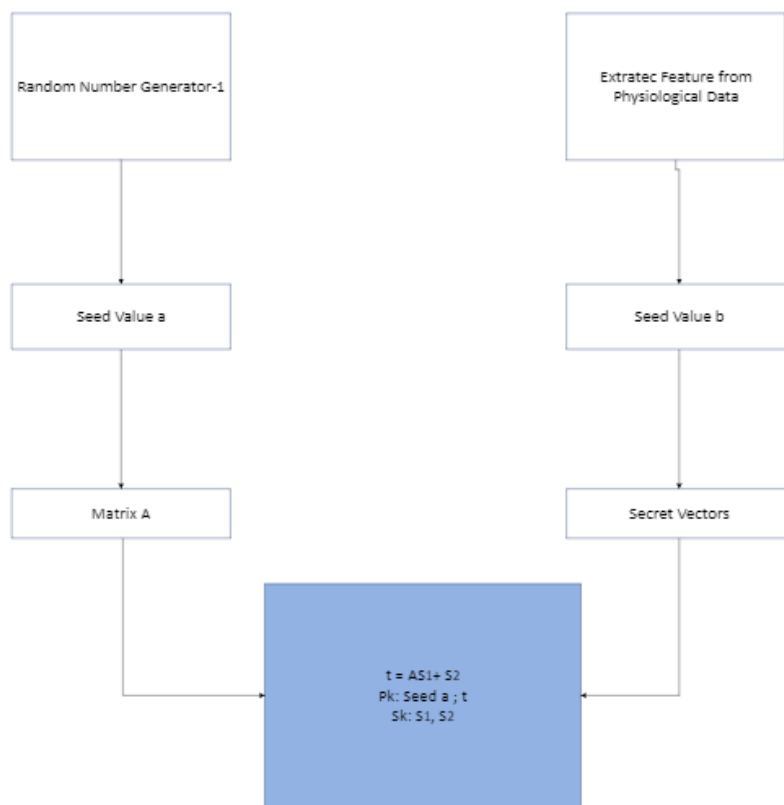


Figure 5.1: KeyGeneration

---

**Algorithm 1:** ECG Feature Detection Algorithm

---

**Data:** ECG signal loaded from a CSV file, Sampling frequency  $F_s$

**Result:** Detected R-peaks, P-waves, T-waves, and QRS complexes

- 1 Load the ECG signal from the input CSV file.
  - 2 Extract the sampling frequency  $F_s$  from the metadata (or define manually if unavailable).
  - 3 Apply a Butterworth bandpass filter to the ECG signal:
  - 4 Cutoff frequencies: 5 Hz to 18 Hz, Filter type: Butterworth (2nd or 4th order).
  - 5 Differentiate the filtered ECG signal to highlight the rapid transitions in QRS complexes.
  - 6 Square the differentiated signal to amplify larger variations and ensure positive values.
  - 7 Smooth the squared signal using a moving average window:
  - 8 Window size: 60 ms (based on  $F_s$ ).
  - 9 Apply moving window integration to the smoothed signal:
  - 10 Window size: 150 ms (based on  $F_s$ ).
  - 11 Initialize signal peaks (SPK) and noise peaks (NPK):
  - 12 SPK represents the amplitude of valid peaks (R-peaks), NPK represents the noise levels.
  - 13 Initialize thresholds Threshold1 and Threshold2.
  - 14 Scan the integrated signal to detect candidate R-peaks:
  - 15 **if** a peak's amplitude exceeds Threshold1 **then**
    - 16     Classify the peak as an R-peak.
    - 17     Update the signal peak (SPK) based on the current R-peak.
    - 18     Recalculate Threshold1 as:
$$\text{Threshold1} = \text{NPK} + 0.25 \times (\text{SPK} - \text{NPK})$$
    - Recalculate Threshold2 for other feature detection.
  - 19 For each detected R-peak, search for the P-wave in a 200 ms window before the R-peak.
  - 20 Search for the T-wave in a 400 ms window after the R-peak.
  - 21 For each detected R-peak, mark the corresponding QRS complex:
  - 22 Start 50 ms before the R-peak, End 100 ms after the R-peak.
  - 23 Plot the original ECG signal with detected features highlighted:
  - 24 Mark R-peaks, P-waves, T-waves, and QRS complexes with different colors.
  - 25 Print the indices or timestamps of the detected R-peaks, P-waves, and T-waves.
  - 26 Optionally save the results to a CSV or text file for further analysis.
-

## 5.1 Kyber Key Generation Algorithm

### Explanation of Steps:

This process creates a pair of keys known as a public key and a private key. The matrix  $A$  and error vectors are created by the seeds given, and public key  $t$  is created from the matrix multiplication and error addition processes. Secret Vectors  $S_1$  and  $S_2$  are generated using physiological data. This approach makes sure that the secret keys and error vectors depend on a unique and specific input from the user which maximize its personalization as well as secure the key generation. The secret vectors and error vectors will be generated based on a specific user's biometric features, which may include a fingerprint, pulse, or other individual characteristics.

---

**Algorithm 2:** KeyGen: An algorithm with caption

---

**Data:** physiological\_seed (optional)

**Result:** pk (Public key), sk (Secret key)

```
1 seed_a ← 48-byte random value using system randomness
2 if physiological_seed is provided then
3   | Use physiological_seed
4 else
5   | physiological_seed ← 48-byte random value
6 Initialize DRBG_a with seed_a
7 Initialize DRBG_b with physiological_seed
8 d ← 32-byte random value using DRBG_a
9 ρ, σ ← G(d)
10 A ← Generate matrix using ρ and DRBG_a
11 s ← Generate secret vector using σ and DRBG_b
12 e ← Generate error vector using σ and DRBG_b
13 t ← A × s + e
14 pk ← Encoded(t) || ρ
15 H(pk) ← Hash of pk
16 sk ← s || pk || H(pk) || Random value z generated by DRBG_a
17 return pk, sk
```

---

## 5.2 Kyber Encapsulation Algorithm

Encapsulation: Encrypts a random message and generates a Shared key that will only be known by both the sender and receiver of the message. The message is included in the formation of the ciphertext from which the shared key is derived from.



---

**Algorithm 3:** Enc: An algorithm with caption

---

**Data:**  $pk$  (Public key),  $key\_length$  (default: 32 bytes)

**Result:**  $c$  (Ciphertext),  $K$  (Shared secret key)

```
1  $m \leftarrow$  Generate 32-byte random message using system randomness
2  $m\_hash \leftarrow H(m)$ 
3  $Kbar, r \leftarrow G(m\_hash \parallel H(pk))$ 
4  $c \leftarrow \text{Encrypt}(m\_hash, r, pk)$ 
5  $K \leftarrow KDF(Kbar \parallel H(c))$ 
6 return  $c, K$ 
```

---

## 5.3 Kyber Decapsulation Algorithm

Decapsulation: Performs the decryption of the ciphertext using the secret key and then check the decrypted message for its validity. If so the shared key is retained otherwise a backup key is created by the variables above matrix.

---

**Algorithm 4:** Dec: Decapsulation Algorithm

---

**Data:**  $c$ : Ciphertext,  $sk$ : Secret key,  $key\_length$ : Desired length of the shared secret key (default: 32 bytes)

**Result:**  $K$ : Shared secret key

```
1  $\_sk, pk, H(pk), z \leftarrow$  Extract components from  $sk$ 
2  $\_m \leftarrow \text{Decrypt}(c, \_sk)$ 
3  $\_Kbar, \_r \leftarrow G(\_m \parallel H(pk))$ 
4  $\_c \leftarrow \text{Encrypt}(\_m\_hash, \_r, pk)$ 
5 if  $\_c = c$  then
6    $K \leftarrow KDF(\_Kbar \parallel H(c))$ 
7 else
8    $K \leftarrow KDF(z \parallel H(c))$ 
9 return  $K$ 
```

---

### Helper Functions

- $xof(bytes32, a, b, length)$ : Expanding function to create output with greater extent than input.
- $h(input\_bytes)$ : The hash function  $H$  to be used is SHA3-256 function.
- $g(input\_bytes)$ : Cryptographic hash function  $G$  that utilizing the SHA3-512 algorithm yields two 32-byte values.

- $\text{prf}(s, b, \text{length})$ : Shake-256 based PRF.
- $\text{kdf}(\text{input\_bytes}, \text{length})$ : Derivation function SHAKE-256 is used as the key derivation function.

## 5.4 Algorithm: Session Key Derivation

AES GCM is used to encrypt the session with the shared key.

---

### Algorithm 5: Session Key Derivation

---

**Data:**

1  $pk, sk, \text{master\_key}$

**Result:**

2  $\text{encrypted\_session\_key}, \text{decrypted\_session\_key}$

3  $(pk, sk) \leftarrow \text{Kyber.keygen}()$

4  $(\text{ciphertext}, \text{shared\_key}) \leftarrow \text{Kyber.enc}(pk)$

5  $\text{decrypted\_key} \leftarrow \text{Kyber.dec}(\text{ciphertext}, sk)$

6  $\text{master\_key} \leftarrow \text{os.urandom}(32)$

7  $\text{session\_key} \leftarrow \text{HKDF}(\text{master\_key})$

8  $\text{nonce} \leftarrow \text{os.urandom}(12)$

9  $(\text{encrypted\_session\_key}, \text{tag}) \leftarrow$   
 $\text{AES-GCM}(\text{session\_key}, \text{shared\_secret}, \text{nonce})$

$\text{decrypted\_session\_key} \leftarrow \text{AES-GCM.decrypt}(\text{encrypted\_session\_key},$   
 $\text{nonce}, \text{tag}, \text{shared\_secret})$

**return**  $\text{encrypted\_session\_key}, \text{decrypted\_session\_key}$

---

# Chapter 6

## ANALYSIS OF THE PROPOSED SYSTEM

### 6.1 Security Analysis

**Quantum Resistance:** The SMA technique is based on Kyber, a KEM that supplies protection against both classical and quantum machines. Kyber's hardness relies on the Learning with Errors (LWE) problem whereby Kyber is resistant to quantum computer attacks such as an attack by Shor's algorithm. This helps in maintaining the security of the encryption scheme even if the adversary has a quantum computing ability.

**Mutual Authentication:** The authentication process involves both the patient and the doctor to ensure that they confirm that the hospital server is genuine, and also the server has to do the same to the patient and the doctor. This eliminates man in the middle attack where an attacker might wish to act like one of the users in order to obtain some precious information.

**Physiological Unclonable Functions (PUFF):** The generation of patient's key pair using PUFFs is also a plus in the overall security. Given that PUFFs are based on the patient's physiological measurements (biometrics), it is almost impossible to counterfeit and as such, the patient's device is protected against hardware control or cloning attacks.

**Patient-Controlled Encryption:** The patient has control over who will have an access to the data that is being collected. In this case, even the data stored in the hospital's dedicated server are encrypted and can only be accessed with explicit permission from the patient to be shared with a medical practitioner. This makes it possible and secure to keep data secret from other people as a way of avoiding insider attacks.

**Protection against Key stolen attack:** The key that is used in secure transaction of the data is actually derived by the patient and encrypt with the shared key. Since the shared key is not actually shared but generated at both end. It protects against

| Element    | Specification |
|------------|---------------|
| System     | Lenovo        |
| Generation | Core i7       |
| RAM        | 4 GB          |
| Processor  | 1700 MHz i    |

**Table 6.1.** System Specification

| Keys Length | Keys Generation  | Encapsulation    | Decapsulation    |
|-------------|------------------|------------------|------------------|
| Kyber 512   | 0.005767 seconds | 0.008305 seconds | 0.013144 seconds |
| Kyber 768   | 0.008511 seconds | 0.011847 seconds | 0.018043 seconds |
| Kyber 1024  | 0.011672 seconds | 0.015547 seconds | 0.024515 seconds |

**Table 6.2.** Performance Table

the shared key stolen attack which is used for the encryption of the session key. This adds the extra layer of the security of session key.

Secure data storage: The data when transferred between patient and the server, it is protected using AES-GCM. A data can be stored at Hospital Server and when that is done the data is further protected by the Hospital Server key HS Enc-Key. Whenever a legitimate user wants the data then first of all it forward the request to the patient and HS will decrypt the data with the help of its HS Enc-Key. After that the encrypted data is transferred to the requestor. The requestor will decrypt the data.

Replay Attack: By deriving session key from master key and by you using additional parameters in KDF such as nonces, salts or context information we ensure that every new and different session key is created and cannot be reused by an attacker.

## 6.2 Performance Analysis

The system specifications for the analysis of protocols are shown in Table 6.1

All times recorded using a Intel Core i7-1255U CPU and averaged over 1000 runs. The values are shown in Table 6.2 and plot in Figure6.1

### Kyber Complexity Analysis

Kyber is a lattice-based cryptographic algorithm that heavily relies on polynomial and matrix operations. The key factors influencing the time complexity are Number-Theoretic Transform (NTT)-based polynomial operations, matrix multiplications, and modular arithmetic.

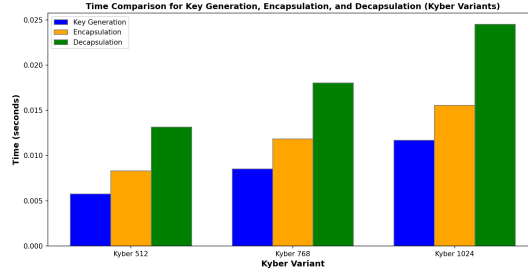


Figure 6.1: Kyber variant Comparison

## Key Components and Complexity

### Polynomial Arithmetic:

Polynomials have degree  $n = 256$  over a field with modulus  $q = 3329$ . Polynomial multiplication uses NTT, with a complexity of  $O(n \log n)$ .

### Matrix Multiplication:

Kyber uses  $k \times k$  matrices, where  $k$  depends on the security level:  $k = 2, 3, 4$  for Kyber512, Kyber768, and Kyber1024, respectively. Matrix multiplication involves polynomials, resulting in a complexity of  $O(k^2 \cdot n \log n)$  due to the NTT-based polynomial multiplication.

### Modular Arithmetic:

Modular reductions on coefficients are  $O(1)$  for each coefficient, yielding a total complexity of  $O(n)$  for polynomials.

## Asymptotic Complexity of Core Operations

### Key Generation Process:

Involves matrix generation ( $O(k^2 \cdot n)$ ), error vector generation ( $O(k \cdot n)$ ), and matrix-vector multiplication ( $O(k^2 \cdot n \log n)$ ).

$$O(k^2 \cdot n \log n)$$

### Encapsulation Process:

Includes matrix transpose generation, error vector generation, matrix-vector multiplication, and polynomial addition.

$$O(k^2 \cdot n \log n)$$

### Decapsulation Process:

Involves vector and polynomial decompression, matrix-vector multiplication, and polynomial subtraction.

$$O(k^2 \cdot n \log n)$$

## Summary of Complexity:

- **Key Generation:**  $O(k^2 \cdot n \log n)$
- **Encryption:**  $O(k^2 \cdot n \log n)$
- **Decryption:**  $O(k^2 \cdot n \log n)$

Where:

- $n = 256$  is the degree of the polynomials.
- $k$  is the number of polynomials ( $k = 2, 3, 4$  for Kyber512, Kyber768, and Kyber1024).

## Scaling with Security Levels:

- Kyber512 ( $k = 2$ ):  $O(4 \cdot n \log n)$
- Kyber768 ( $k = 3$ ):  $O(9 \cdot n \log n)$
- Kyber1024 ( $k = 4$ ):  $O(16 \cdot n \log n)$

As the security level increases, the complexity scales quadratically ( $k^2$ ), with computational costs roughly quadrupling for each increment in  $k$ .

# Chapter 7

## SUMMARY OF RESEARCH WORK

This work revolves around the improvement of post-quantum cryptography on patient data security and privacy in hospital contexts. The following solution involves the use of quantum-resistant cryptography known as the Kyber-based key encapsulation mechanism (KEM) in performing mutual authentication between a patient, a doctor, and a hospital server. The main goal is to preserve the confidentiality and integrity of medical information and provide secure communication given that new quantum computing threats.

**Key Components of the System:** **Patient:** The person of interest whose medical record information is being collected, analyzed and being accessed. They employ a personal device (wearable sensor) to engage with the hospital's systems.

**Doctor:** The healthcare provider who needs secure access to the patient's medical records for accurate diagnosing and constant assessment.

**Hospital Server:** The main server through which patient information is stored.

The system uses Kyber based key generation, to generate the shared secret, between the patient's device and the hospital server and between the doctor's device and the hospital server. The process starts with the patient and the hospital server creating their own Kyber key pairs which are exchanged securely. In this method, challenge-response is employed to derive a session key and verify the patient and the hospital server. The same process is repeated by the doctor with the hospital's server.

After authentication is done, a session key is created and the doctor has access to the patient's data in encrypted form. The patient has complete authority over his/her data, deciding whether or not someone can view it. This is achieved through the encryption of a temporary access key using the doctor's public key. The doctor can therefore decipher the access key to gain full access to the information for some time as the patients hold the authority over their records.

The implementation of the proposed system therefore involves the development of a novel way of implementing a mutual authentication that is not vulnerable to post

quantum process attacks, an essential security measure given the increasingly insecure hospital settings preserving the privacy of medical information. The use of Kyber algorithm, which is a post-quantum cryptographic scheme means that the patient data is safe from the potential threats posed by quantum computers hence providing long term security for patients information. Every interaction in the form of a communication session between the parties: patients, doctors and hospital servers is assigned a new, temporary Session ID which is then deleted, thus eliminating threats from the reuse of keys and replay-attacks. The design ensures that the session keys cannot be repeated again, thus reducing on the vulnerabilities and ensuring on the session or communication integrity on a given network. Also, it allows patients to set permissions on their data so that only enhancing medical personnel with the patient's permission can access the data. Digital data is protected through use of encryptions using session keys so that only the intended recipient can be in a position to decode it.

The system effectively addresses several critical challenges: it minimizes key reuse, provides forward security where the exposure of one session key does not compromise others, and offers quantum-safe authentication to counter subsequent security threats. As for the future work, there could be a number of improvement: one option is to incorporate a key recovery or key escrow service which allows to access the data after the session key expiration. All in all, the proposed solution exhibits a deep level of security and a high degree of scalability, which make the data more secure and the control over medical information more effective in the context of the continuously developing cryptographic technologies.



# Chapter 8

## CONCLUSION

### 8.1 Conclusion

In this thesis, we presented the development of a Keys generation and establishment system for Post-Quantum Cryptography for the hospital environment where patient information is vulnerable to hacking and unauthorized access. The system implemented security that protect patients, doctors, and confidentiality of the hospitals, servers through Kyber-based key encapsulation mechanisms (KEM), which is a quantum-safe cryptographic algorithm that guards against security threats from future foam quantum computing. Yet another strength of this system is patient control over privacy since only specific health care personnel who have the consent of the patient is permitted to access the patient's records.

One additional feature of this system is the creation of Kyber key pairs from physiological data of a patient by employing PUFFs. Every time a new authentication session is to commence, a new key pair is then produced from the patient's physiological parameters (biometric). This approach also helps for binding the patient's cryptographic identification to their physiological data; making the further tamper-proof and immune to impersonation or cloning attacks. Employment of temporary keys generated from physiological data ensures that the session key between the patient, doctor, and the hospital server is a unique key and the key is deconstructed after the particular session.

The system strengths are its capability of providing quantum resistant encryption, session key and patient controlled access. To mitigate this risk the system implements post-quantum cryptographic algorithms for instance Kyber, which help in protecting the privacy of the medical data in the system against likely quantum computing attacks. However, when physiological data is used for key generation, there is an added element of security because the patient's keys cannot be easily duplicated or breached.

However, the system serves as a good solution to many pressing security issues, but there are some areas of weakness that needs to be discussed. The current system assigns the tasks of managing session key recovery to the patient’s device, which seems to increase the burden on the patient.

## 8.2 Future Work

Nonetheless, since the proposed system will improve many security issues prevalent in hospitals, some aspects of the system require more research and development aimed at improving the system’s functionality, security, and usability. One of the possible enhancements is the integration of enhanced key recovery mechanisms. As of now, session keys are temporary and are deleted once a session is over, which may cause difficulties for a patient who needs to remember the context. To reduce the stress of key recovery from the side of the patient, one can consider the use of a key recovery or key escrow system; it is also possible to tighten access controls to the extracted keys to prevent unauthorized access. This would make it possible to allow access to information that is supposed to be available, for instance, to doctors without comprising on the privacy and security of the patient’s information.

Adopting techniques such as homomorphic encryption could also add another layer to data protection since the data can be computationally analyzed in an encrypted form. Such an approach would allow doctors for instance to carry out operations on the data such as analytics and anomaly detections with the data being encrypted thereby maintaining the privacy of patients’ information. Furthermore, the performance enhancement studies of post-quantum cryptographic algorithms are also needed; particularly for constrained devices such as Wearable sensors and Smartphones. There is a need for future studies to work towards minimizing computational burden and consumption in an effort to make post-quantum security a realizable possibility in different devices.

In another area, it is possible to speak about the enhancement of the patient consent mechanisms. The current system enables patient to specify either full consent or no consent to the access of data correlated to them but more refined mechanisms of consent could allow the patient to determine in detail which data (say records or time periods) can be shared with the healthcare providers. Real-time notifications of the data access and approval mechanisms through the mobile applications could also improve the patient control functions sentimental in the case of emergency or ongoing care management.

In conclusion, despite the fact that the proposed system is very effective in ensuring the quantum-resistant mutual authentication for the healthcare sector, there is a

lot of research that needs to be carried out with regards to the process of key management, the user-friendliness of the system as well as better cryptographic approaches. Additional features including proxy re-encryption, Homomorphic encryption and Integration of block chain along with a better mechanism to obtain the consent of the patient will make the system more robust and suitable for real time implementation in the hospital environment to provide a long-term security for the valuable medical data.

# Bibliography

- [1] Nima Karimian, Zimu Guo, Mark Tehranipoor, and Domenic Forte. Highly reliable key generation from electrocardiogram (ecg). *IEEE Transactions on Biomedical Engineering*, 64(6):1400–1411, 2016.
- [2] Duygu Karaođlan Altop, Albert Levi, and Volkan Tuzcu. Towards using physiological signals as cryptographic keys in body area networks. In *2015 9th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth)*, pages 92–99. IEEE, 2015.
- [3] Jongseok Ryu, Jihyeon Oh, Deokkyu Kwon, Seunghwan Son, Joonyoung Lee, Yohan Park, and Youngho Park. Secure ecc-based three-factor mutual authentication protocol for telecare medical information system. *IEEE Access*, 10:11511–11526, 2022.
- [4] Prosanta Gope and Tzonelih Hwang. Bsn-care: A secure iot-based modern healthcare system using body sensor network. *IEEE sensors journal*, 16(5):1368–1376, 2015.
- [5] Prosanta Gope, Youcef Gheraibia, Sohag Kabir, and Biplab Sikdar. A secure iot-based modern healthcare system with fault-tolerant decision making process. *IEEE Journal of Biomedical and Health Informatics*, 25(3):862–873, 2020.
- [6] Omar Ibrahim Obaid and Saba Abdul-Baqi Salman. Security and privacy in iot-based healthcare systems: a review. *Mesopotamian Journal of Computer Science*, 2022:29–39, 2022.
- [7] Vincent Liu, Mark A Musen, and Timothy Chou. Data breaches of protected health information in the united states. *Jama*, 313(14):1471–1473, 2015.
- [8] Maxim Chernyshev, Sherali Zeadally, and Zubair Baig. Healthcare data breaches: Implications for digital forensic readiness. *Journal of medical systems*, 43:1–12, 2019.
- [9] GetAstra. Healthcare data breach statistics, 2022.

- [10] Ibrahim Sadek, Josué Codjo, Shafiq Ul Rehman, and Bessam Abdulrazak. Security and privacy in the internet of things healthcare systems: Toward a robust solution in real-life deployment. *Computer Methods and Programs in Biomedicine Update*, 2:100071, 2022.
- [11] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, 1(2-3):293–315, 2003.
- [12] Linus Wallgren, Shahid Raza, and Thiemo Voigt. Routing attacks and countermeasures in the rpl-based internet of things. *International Journal of Distributed Sensor Networks*, 9(8):794326, 2013.
- [13] JX Zhang and K Hoshino. Chapter 8—implantable and wearable sensors. *Micro and Nano Technologies; Academic Press: Cambridge, MA, USA*, pages 489–545, 2019.
- [14] Xin Xu, Zheng Ping Jin, Hua Zhang, and Ping Zhu. A dynamic id-based authentication scheme based on ecc for telecare medicine information systems. *Applied Mechanics and Materials*, 457:861–866, 2014.
- [15] Sk Hafizul Islam and Muhammad Khurram Khan. Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems. *Journal of medical systems*, 38(10):135, 2014.
- [16] Shehzad Chaudhry, Syed Naqvi, Taeshik Shon, Muhammad Sher Ramzan, and Mohammad Farash. Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems. *Journal of Medical Systems*, 39, 04 2015.
- [17] Shuming Qiu, Guoai Xu, Haseeb Ahmad, and Licheng Wang. A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems. *IEEE access*, 6:7452–7463, 2017.
- [18] Benjamin Talbot, Sara Farnbach, Allison Tong, Steve Chadban, Shaundee Sen, Vincent Garvey, Martin Gallagher, and John Knight. Patient and clinician perspectives on the use of remote patient monitoring in peritoneal dialysis. *Canadian Journal of Kidney Health and Disease*, 9:20543581221084499, 2022.
- [19] Carmen CY Poon, Yuan-Ting Zhang, and Shu-Di Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, 44(4):73–81, 2006.
- [20] Kegomoditswe Boikanyo, Adamu Murtala Zungeru, Boyce Sigweni, Abid Yahya, and Caspar Lebekwe. Remote patient monitoring systems: Applications, architecture, and challenges. *Scientific African*, 20:e01638, 2023.

- [21] David Whitehead and Jared Conley. The next frontier of remote patient monitoring: hospital at home. *Journal of Medical Internet Research*, 25:e42335, 2023.
- [22] M Jamal Deen. Information and communications technologies for elderly ubiquitous healthcare in a smart home. *Personal and Ubiquitous Computing*, 19:573–599, 2015.
- [23] Azra Hazwanie Azizulkarim, Muhammad Mahadi Abdul Jamil, and Radzi Ambar. Design and development of patient monitoring system. In *IOP Conference Series: Materials Science and Engineering*, volume 226, page 012094. IOP Publishing, 2017.
- [24] Sumit Majumder, Tapas Mondal, and M Jamal Deen. Wearable sensors for remote health monitoring. *Sensors*, 17(1):130, 2017.
- [25] Timothy Malche, Sumegh Tharewal, Pradeep Kumar Tiwari, Mohamed Yaseen Jabarulla, Abeer Ali Alnuaim, Wesam Atef Hatamleh, and Mohammad Aman Ullah. [retracted] artificial intelligence of things-(aiot-) based patient activity tracking system for remote patient monitoring. *Journal of Healthcare Engineering*, 2022(1):8732213, 2022.
- [26] H Fouad, Azza S Hassanein, Ahmed M Soliman, and Haytham Al-Feel. Analyzing patient health information based on iot sensor with ai for improving patient assistance in the future direction. *Measurement*, 159:107757, 2020.
- [27] Anu Bhargava and Mike Zoltowski. Sensors and wireless communication for medical care. In *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.*, pages 956–960. IEEE, 2003.
- [28] Nivedita James Palatty. 80+ healthcare data breach statistics 2024, December 2023. Updated statistics on healthcare data breaches.
- [29] Steve Alder. Healthcare data breach statistics. August 2024. Posted online.
- [30] Marcus de Ree, Damian Vizar, Georgios Mantas, Joaquim Bastos, Corinne Kassapoglou-Faist, and Jonathan Rodriguez. A key management framework to secure iomt-enabled healthcare systems. pages 1–6, 10 2021.
- [31] Muhamed Turkanović, Boštjan Brumen, and Marko Hölbl. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. *Ad Hoc Networks*, 20:96–112, 2014.
- [32] Ruhul Amin, SK Hafizul Islam, GP Biswas, Muhammad Khurram Khan, Lu Leng, and Neeraj Kumar. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer Networks*, 101:42–62, 2016.

- [33] Shantanu Pal, Michael Hitchens, Vijay Varadharajan, and Tahiry Rabehaja. Policy-based access control for constrained healthcare resources in the context of the internet of things. *Journal of Network and Computer Applications*, 139:57–74, 2019.
- [34] Abdulatif Alabdulatif, Ibrahim Khalil, Xun Yi, and Mohsen Guizani. Secure edge of things for smart healthcare surveillance framework. *IEEE access*, 7:31010–31021, 2019.
- [35] Geeta Sharma and Sheetal Kalra. A lightweight user authentication scheme for cloud-iot based healthcare services. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, 43:619–636, 2019.
- [36] Preeti Chandrakar, Sonam Sinha, and Rifaqat Ali. Cloud-based authenticated protocol for healthcare monitoring system. *Journal of Ambient Intelligence and Humanized Computing*, 11:3431–3447, 2020.
- [37] Lu Zhou, Xiong Li, Kuo-Hui Yeh, Chunhua Su, and Wayne Chiu. Lightweight iot-based authentication scheme in cloud computing circumstance. *Future generation computer systems*, 91:244–251, 2019.
- [38] Mohammad Sabzinejad Farash, Muhamed Turkanović, Saru Kumari, and Marko Hölbl. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. *Ad Hoc Networks*, 36:152–176, 2016.
- [39] Goutam Tamvada and Sofía Celi. Deep dive into a post-quantum key encapsulation algorithm. 2022.
- [40] Ruben Gonzalez. Kyber - how does it work?, September 2021.
- [41] Sanaz Rahimi Moosavi. Ppg-keygen: Using photoplethysmogram for key generation in wearable devices. *Procedia Computer Science*, 184:291–298, 2021.
- [42] Weiguo Sheng, Gareth Howells, Michael Fairhurst, Farzin Deravi, and Shengyong Chen. Reliable and secure encryption key generation from fingerprints. *Information Management & Computer Security*, 20(3):207–221, 2012.
- [43] S Nagaraju, R Nagendra, Shanmugham Balasundaram, and R Kiran Kumar. Biometric key generation and multi round aes crypto system for improved security. *Measurement: Sensors*, 30:100931, 2023.
- [44] Pinki Kumari and Abhishek Vaish. Brainwave based user identification system: A pilot study in robotics environment. *Robotics and Autonomous Systems*, 65:15–23, 2015.

- [45] Junqing Zhang, Yushi Zheng, Weitao Xu, and Yingying Chen. H2k: A heartbeat-based key generation framework for ecg and ppg signals. *IEEE Transactions on Mobile Computing*, 2021.
- [46] Jagadeeswararao Annam, Suja Radha, Jayaprada Somala, Dr Prasad, Narayana Satyala, and Bapi Surampudi. *ECG Feature Extraction*, pages 177–195. 01 2022.
- [47] Putri Madona, Rahmat Ilias Basti, and Muhammad Mahrus Zain. Pqrst wave detection on ecg signals. *Gaceta sanitaria*, 35:S364–S369, 2021.
- [48] Anupreet Kaur Singh and Sridhar Krishnan. Ecg signal feature extraction trends in methods and applications. *BioMedical Engineering OnLine*, 22(1):22, 2023.
- [49] M Ramkumar, C Ganesh Babu, S Karthikeyani, GS Priyanka, and R Sarath Kumar. Probabilistic feature extraction techniques for electrocardiogram signal-a review. In *IOP Conference Series: Materials Science and Engineering*, volume 1084, page 012024. IOP Publishing, 2021.
- [50] Abdullah Alhayajneh, Alessandro N Baccarini, Gary M Weiss, Thaier Hayajneh, and Aydin Farajidavar. Biometric authentication and verification for medical cyber physical systems. *Electronics*, 7(12):436, 2018.
- [51] Md Niaz Imtiaz and Naimul Khan. Pan-tompkins++: A robust approach to detect r-peaks in ecg signals. In *2022 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, pages 2905–2912. IEEE, 2022.



# Appendix A

## CODE IMPLEMENTATION

### A.0.1 Loading and Preprocessing the ECG Signal

```
import numpy as np
import pandas as pd
import scipy.signal as signal
import matplotlib.pyplot as plt

# Load the CSV file
ReadFile = pd.read_csv('FilePath')
ecg_signal = pd.to_numeric(ReadFile['ECG_LARA_24BIT_CAL'],
errors='coerce').values
ecg_signal = ecg_signal[~np.isnan(ecg_signal)] # Remove NaN values
# Bandpass filter with passband of 5-18 Hz
b, a = signal.butter(1, [5 / 250, 18 / 250], btype='band')
filtered_ecg = signal.lfilter(b, a, ecg_signal)
# Differentiate the signal\
diff_ecg = np.diff(filtered_ecg)

# Perform point-by-point squaring
squared_ecg = diff_ecg ** 2

# Smooth the signal using a 60ms wide flattop window
window_size_smooth = int(0.06 * 250) # 60 ms window
flattop_window = np.ones(window_size_smooth)
smoothed_ecg = np.convolve(squared_ecg, flattop_window, mode='same')

# Apply moving window integration with a 150ms wide window
window_size_integration = int(0.15 * 250) # 150 ms window
```

```
integrated_ecg = np.convolve(smoothed_ecg,  
np.ones(window_size_integration) / window_size_integration, mode='same')
```

## A.0.2 Plotting the ECG Signals

```
# Plot intermediate signals for verification  
plt.figure(figsize=(18, 12))  
  
plt.subplot(4, 1, 1)  
plt.plot(ecg_signal)  
plt.title("Original ECG Signal")  
  
plt.subplot(4, 1, 2)  
plt.plot(filtered_ecg)  
plt.title("Filtered ECG Signal (5-18 Hz Bandpass)")  
  
plt.subplot(4, 1, 3)  
plt.plot(integrated_ecg)  
plt.title("Integrated ECG Signal")  
  
plt.tight_layout()  
plt.show()
```

## A.0.3 R-Peak Detection and Threshold Calculation

```
# Decision Phase  
# Set very sensitive thresholds and smaller distance  
peak_indices,properties = signal.find_peaks(integrated_ecg,  
distance=int(0.15*250),  
height=np.mean(integrated_ecg) * 0.1)  
  
# Initialize thresholds  
SPK = np.max(integrated_ecg) # Initial guess for signal peak  
NPK = np.min(integrated_ecg) # Initial guess for noise peak  
Threshold1 = NPK + 0.02 * (SPK - NPK) # Very sensitive threshold  
Threshold2 = 0.4 * Threshold1
```

## A.0.4 Feature Detection: P-Waves and T-Waves

```
# P and T Wave Detection:
```

```

for r_peak in R_peaks:
    # Search for P wave before the R peak within 200 ms window
    p_wave_search_start = max(0, r_peak - int(0.2 * 250))
    p_wave_search_end = r_peak
    p_wave_index = np.argmin(filtered_ecg[p_wave_search_start:
    p_wave_search_end]) + p_wave_search_start
    P_waves.append(p_wave_index)

    # Search for T wave after the R peak within 400 ms window
    t_wave_search_start = r_peak
    t_wave_search_end = min(len(filtered_ecg), r_peak + int(0.4 * 250))
    t_wave_index = np.argmax(
filtered_ecg[t_wave_search_start:t_wave_search_end])
+ t_wave_search_start
    T_waves.append(t_wave_index)

```

### A.0.5 Plotting Detected Features

```

# Plotting the ECG Signal with Detected Features (R-Peaks, P Waves, T Waves)
plt.figure(figsize=(18, 12))

plt.subplot(2, 1, 1)
plt.plot(ecg_signal, label='ECG Signal with Detected Features')
plt.scatter(R_peaks, ecg_signal[R_peaks],
color='red', label='Detected R-Peaks')
plt.scatter(P_waves, ecg_signal[P_waves],
color='blue', label='Detected P Waves')
plt.scatter(T_waves, ecg_signal[T_waves],
color='green', label='Detected T Waves')

# Mark QRS Complexes
for r_peak in R_peaks:
    qrs_start = max(0, r_peak - int(0.05 * 250))
    # QRS complex typically starts ~50ms before R-peak
    qrs_end = min(len(ecg_signal), r_peak + int(0.1 * 250))
    # QRS complex typically ends ~100ms after R-peak
    plt.axvspan(qrs_start, qrs_end, color='yellow',
alpha=0.3, label='QRS Complex' if r_peak == R_peaks[0] else "")

plt.title("ECGSignal with Detected R-Peaks,P Waves, T Waves, and QRS Complexes")
plt.xlabel("Sample Number")

```

```

plt.ylabel("Amplitude")
plt.legend()

plt.tight_layout()
plt.show()

print(f"R-peaks: {R_peaks}")
print(f"P-waves: {P_waves}")
print(f"T-waves: {T_waves}")

# Combine extracted features (P, R, T peaks) into a feature vector
features = np.array(R_peaks + P_waves + T_waves)

# Define a random projection matrix to apply a non-invertible transformation
def generate_random_projection_matrix(size):
    return np.random.randn(size, size)

# Apply a random projection (non-invertible transformation)
def apply_cancelable_transformation(features, projection_matrix):
    return np.dot(projection_matrix, features)

# Generate a random projection matrix for transformation
random_projection_matrix = generate_random_projection_matrix(len(features))

# Apply transformation to features
cancelable_template =
apply_cancelable_transformation(features, random_projection_matrix)

# Normalize cancelable template for visualization

cancelable_template_normalized =

```

```

(cancelable_template - np.min(cancelable_template)) /

(np.max(cancelable_template) - np.min(cancelable_template))

cancelable_template_normalized, delimiter=',')

# Plot the Cancelable Template
plt.figure(figsize=(12, 6))
plt.plot(cancelable_template_normalized, label='Cancelable Template')
plt.title("Cancelable Template Generated from ECG Features")
plt.xlabel("Transformed Feature Index")
plt.ylabel("Normalized Value")
plt.legend()
plt.show()

# Print the generated cancelable template
print("Cancelable Template:", cancelable_template_normalized)

```

## Appendix B

```
import os
import hashlib
from hashlib import sha3_256, sha3_512, shake_128, shake_256
from polynomials import * # Assume you have polynomials, modules, and ntt_helper
from modules import *
from ntt_helper import NTTHelperKyber
```

```
DEFAULT_PARAMETERS = {
    "kyber_512": {
        "n": 256,
        "k": 2,
        "q": 3329,
        "eta_1": 3,
        "eta_2": 2,
        "du": 10,
        "dv": 4,
    },
    "kyber_768": {
        "n": 256,
        "k": 3,
        "q": 3329,
        "eta_1": 2,
        "eta_2": 2,
        "du": 10,
        "dv": 4,
    },
    "kyber_1024": {
        "n": 256,
        "k": 4,
        "q": 3329,
        "eta_1": 2,
        "eta_2": 2,
        "du": 11,
        "dv": 5,
    }
}
```

```

class Kyber:
    def __init__(self, parameter_set):
        self.n = parameter_set["n"]
        self.k = parameter_set["k"]
        self.q = parameter_set["q"]
        self.eta_1 = parameter_set["eta_1"]
        self.eta_2 = parameter_set["eta_2"]
        self.du = parameter_set["du"]
        self.dv = parameter_set["dv"]

        self.R = PolynomialRing(self.q, self.n, ntt_helper=NTTHelperKyber)
        self.M = Module(self.R)

        self.drbg_a = None
        self.drbg_b = None

    def set_drbg_seed_a(self, seed_a):
        """Set DRBG for generating matrix A."""
        self.drbg_a = AES256_CTR_DRBG(seed_a)

    def set_drbg_seed_b(self, seed_b):

        self.drbg_b = AES256_CTR_DRBG(seed_b)

    def random_bytes_a(self, length):
        if self.drbg_a:
            return self.drbg_a.random_bytes(length)
        else:
            return os.urandom(length)

    def random_bytes_b(self, length):
        if self.drbg_b:
            return self.drbg_b.random_bytes(length)
        else:
            return os.urandom(length)

    @staticmethod
    def _xof(bytes32, a, b, length):
        input_bytes = bytes32 + a + b
        if len(input_bytes) != 34:
            raise ValueError("Input bytes should be one 32 byte array

```

```

and 2 single bytes.")
    return shake_128(input_bytes).digest(length)

    @staticmethod
    def _h(input_bytes):

        return sha3_256(input_bytes).digest()

    @staticmethod
    def _g(input_bytes):

        output = sha3_512(input_bytes).digest()
        return output[:32], output[32:]

    @staticmethod
    def _prf(s, b, length):

        input_bytes = s + b
        if len(input_bytes) != 33:
            raise ValueError("Input bytes should be one 32 byte array
            and one single byte.")
        return shake_256(input_bytes).digest(length)

    @staticmethod
    def _kdf(input_bytes, length):

        return shake_256(input_bytes).digest(length)

def _generate_error_vector(self, sigma, eta, N, is_ntt=False):

    elements = []
    for i in range(self.k):
        input_bytes = self._prf(sigma, bytes([N]), 64 * eta)
        poly = self.R.cbd(input_bytes, eta, is_ntt=is_ntt)
        elements.append(poly)
        N += 1
    v = self.M(elements).transpose()
    return v, N

def _generate_matrix_from_seed(self, rho, transpose=False, is_ntt=False):

```



```

    A = []
    for i in range(self.k):
        row = []
        for j in range(self.k):
            if transpose:
                input_bytes = self._xof(rho, bytes([i]), bytes([j]),
3 * self.R.n)
            else:
                input_bytes = self._xof(rho, bytes([j]), bytes([i]),
3 * self.R.n)
            aij = self.R.parse(input_bytes, is_ntt=is_ntt)
            row.append(aij)
        A.append(row)
    return self.M(A)

def _cpapke_keygen(self, seed_a, seed_b):

    # Generate random value d for matrix A
    d = self.random_bytes_a(32)
    rho, sigma = self._g(d)
    N = 0

    # Generate matrix A using seed_a
    A = self._generate_matrix_from_seed(rho, is_ntt=True)

    # Generate error vector s using seed_b
    s, N = self._generate_error_vector(sigma, self.eta_1, N)
    s.to_ntt()

    # Generate error vector e using seed_b
    e, N = self._generate_error_vector(sigma, self.eta_1, N)
    e.to_ntt()

    # Construct the public key
    t = (A @ s).to_montgomery() + e

    # Reduce vectors mod q
    t.reduce_coefficients()
    s.reduce_coefficients()

    # Encode elements to bytes and return

```

```

pk = t.encode(l=12) + rho
sk = s.encode(l=12)
return pk, sk

def _cpapke_enc(self, pk, m, coins):

    N = 0
    rho = pk[-32:] # Last 32 bytes of the public key is rho

    tt = self.M.decode(pk, 1, self.k, l=12, is_ntt=True)

    # Encode message as polynomial
    m_poly = self.R.decode(m, l=1).decompress(1)

    # Generate the matrix  $A^T R^{(kxk)}$ 
    At = self._generate_matrix_from_seed(rho, transpose=True, is_ntt=True)

    # Generate the error vector  $r R^k$ 
    r, N = self._generate_error_vector(coins, self.eta_1, N)
    r.to_ntt()

    e1, N = self._generate_error_vector(coins, self.eta_2, N)

    input_bytes = self._prf(coins, bytes([N]), 64 * self.eta_2)
    e2 = self.R.cbd(input_bytes, self.eta_2)
    u = (At @ r).from_ntt() + e1
    v = (tt @ r)[0][0].from_ntt()
    v = v + e2 + m_poly

    # Ciphertext to bytes
    c1 = u.compress(self.du).encode(l=self.du)
    c2 = v.compress(self.dv).encode(l=self.dv)

    return c1 + c2

def _cpapke_dec(self, sk, c):

```

```

index = self.du * self.k * self.R.n // 8
c1 = c[:index]
c2 = c[index:]

# Recover the vector u and convert to NTT form
u = self.M.decode(c1, self.k, 1, l=self.du).decompress(self.du)
u.to_ntt()

# Recover the polynomial v
v = self.R.decode(c2, l=self.dv).decompress(self.dv)

# s_transpose (already in NTT form)
st = self.M.decode(sk, 1, self.k, l=12, is_ntt=True)

# Recover message as polynomial
m = (st @ u)[0][0].from_ntt()
m = v - m

# Return message as bytes
return m.compress(1).encode(l=1)

def keygen(self):

    seed_a = os.urandom(48)
    seed_b = os.urandom(48)
    self.set_drbg_seed_a(seed_a)
    self.set_drbg_seed_b(seed_b)

    # Generate keys with two seeds
    pk, _sk = self._cpapke_keygen(seed_a, seed_b)
    z = self.random_bytes_a(32) # Use first RNG for z

    # sk = sk' || pk || H(pk) || z
    sk = _sk + pk + self._h(pk) + z
    return pk, sk

def enc(self, pk, key_length=32):

    m = os.urandom(32) # Randomly generated 32-byte message
    m_hash = self._h(m)
    Kbar, r = self._g(m_hash + self._h(pk))

```

```

        c = self._cpapke_enc(pk, m_hash, r) # Encrypt the message
        K = self._kdf(Kbar + self._h(c), key_length) # Derive the shared key
        return c, K

def dec(self, c, sk, key_length=32):

    index = 12 * self.k * self.R.n // 8
    _sk = sk[:index]
    pk = sk[index:-64]
    hpk = sk[-64:-32]
    z = sk[-32:]

    # Decrypt the ciphertext
    _m = self._cpapke_dec(_sk, c)

    # Decapsulation
    _Kbar, _r = self._g(_m + hpk)
    _c = self._cpapke_enc(pk, _m, _r)
    if _c == c:
        K = self._kdf(_Kbar + self._h(c), key_length)
    else:
        K = self._kdf(z + self._h(c), key_length)
    return K

# Initialise with default parameters for easy import
Kyber512 = Kyber(DEFAULT_PARAMETERS["kyber_512"])
Kyber768 = Kyber(DEFAULT_PARAMETERS["kyber_768"])
Kyber1024 = Kyber(DEFAULT_PARAMETERS["kyber_1024"])

from kyber import Kyber, DEFAULT_PARAMETERS
import os

def perform_kyber_operations(kyber, kyber_name):
    # Generate key pair
    public_key, secret_key = kyber.keygen()
    print(f"{kyber_name} Public Key (Hex):", public_key)
    print(f"{kyber_name} Secret Key (Hex):", secret_key.hex())

    # Encrypt a message
    ciphertext, shared_key = kyber.enc(public_key)

```

```

print(f"{kyber_name} Ciphertext (Hex):", ciphertext.hex())
print(f"{kyber_name} Shared Key (Hex):", shared_key.hex())

# Decrypt the ciphertext
decrypted_key = kyber.dec(ciphertext, secret_key)
print(f"{kyber_name} Decrypted Key (Hex):", decrypted_key.hex())

# Verify that the decrypted key matches the shared key
if shared_key == decrypted_key:
    print(f"{kyber_name} Key successfully decrypted
        and matches the shared key.")
else:
    print(f"{kyber_name} Decrypted key does not match the shared key.")

def main():
    # Perform operations for Kyber 512
    kyber512 = Kyber(DEFAULT_PARAMETERS["kyber_512"])
    perform_kyber_operations(kyber512, "Kyber 512")

    # Perform operations for Kyber 768
    kyber768 = Kyber(DEFAULT_PARAMETERS["kyber_768"])
    perform_kyber_operations(kyber768, "Kyber 768")

    kyber768 = Kyber(DEFAULT_PARAMETERS["kyber_1024"])
    perform_kyber_operations(kyber768, "Kyber 1024")

    # kyber1024 = Kyber(DEFAULT_PARAMETERS["kyber_1024"])
    # perform_kyber_operations(kyber1024, "Kyber 1024")

if __name__ == "__main__":
    main()

```