DEMOCRATIC REPUBLIC OF ALGERIA PEOPLE

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

UNIVERSITY MOHAMED BOUDIAF - M'SILA

FACULTY: Mathematics and Informatic

DEPARTEMENT of computer science

N° : ……..

DOMAIN: Mathematics and Informatics

BRANCH: Computer Science

OPTION: RTIC

A Dissertation in Fulfillment

For the Requirement of the Degree of MASTER

By: BACHIRI Achouak || LEMOUNES Ahlam

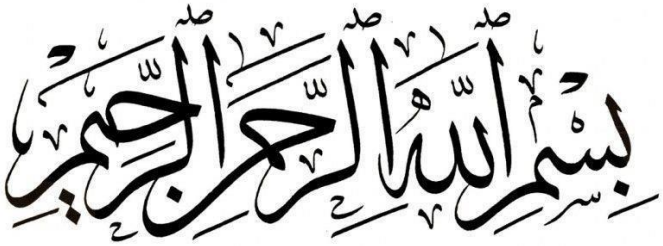
Subject:

Authentication Scheme using RFID for Healthcare Applications

Defended to the jury:

Dr. Mohemed Benouis	University of M’sila	Chairman
Dr. Noureddine Chikouche	University of M’sila	Supervisor
Dr. Fares Mezrag	University of M’sila	Examiner

Academic year: 2021 / 2022


بسم الله الرحمن الرحيم

Acknowledgements

I would like to express my deep and sincere gratitude to my research supervisor: Dr. CHIKOUCHE Noureddine for give me the opportunity to conduct research and provide invaluable information throughout this research. I was inspired by his dynamism, vision, dedication, motivation and his own diligence. I am very grateful for what he provided to us.

I would also like to thank Dr. Hamza Rafik for what he taught me how to conduct research and present research work as clearly as possible and for his friendship, sympathy, and good sense of humor.

To our families to their endless love, support and encouragement.

Dedication

First of all, thanks and praise be to God Almighty for my success during my research work to complete the research successfully.

I'm very grateful to my parents for their love, prayers, care and sacrifices to educate me and prepare me for my future.

I also express my thanks to my sister Dallal for her support and valuable prayers.

BACHIRI Achouak

Dedication

After a long and long wait, we waited behind the school benches; we stand at the threshold of graduation and declare our longing for the weapon of creativity, excellence, determination and success.

From here, I dedicate this graduation to the soul of my dear father, may God have mercy on him, and make him one of the people of Paradise, and to my dear mother, this is how you wanted me to be, and this is how I follow your path always and forever.

And to my dear brothers and teachers, from the beginning of the journey until this beautiful moment, and I thank everyone who stood with me and supported me throughout my academic path, and I congratulate all my friends who graduated with me, and I congratulate their families, and God willing, the appointment to serve our dear country.

LEMOUNES Ahlam

ABSTRACT

Radio frequency identification (RFID) technology has been used to build improved healthcare systems in recent years, providing a variety of healthcare services that can benefit both medical staff and patients. However, because RFID systems use unsecure communication routes, security is a major concern that must be addressed before RFID can be deployed in healthcare systems. The major goal of this project is to develop a better RFID authentication protocol that ensures security. We improved a pervious Protocol Agrahari et al. that was based on ECQV with a new algorithm kyber.CPA PKE that considered as a candidate in NIST post-quantum cryptography standardization NIST post-quantum cryptography standardization. We used kyber.CPA PKE which consisting of key generation, encryption and decryption algorithm for achieve our goal and to overcome these weaknesses that existing before. The security of our scheme is confirmed with security analyses Based on several metrics. Besides, it is compatible with low-cost RFID tags. Moreover, our protocol achieves better performance and it fulfils the basic requirements. Thus, the suggested protocol is capable of providing excellent security for RFID-based healthcare systems.

Key words: Authentication, healthcare system, RFID, security.

ملخص

تم استخدام تقنية تحديد الترددات الراديوية (RFID) لبناء أنظمة رعاية صحية محسنة في السنوات الأخيرة، مما يوفر مجموعة متنوعة من خدمات الرعاية الصحية التي يمكن أن تفيد كلاً من الطاقم الطبي والمرضى. ومع ذلك، نظرًا لأن أنظمة RFIDتستخدم طرق اتصال غير آمنة، فإن الأمن يمثل مصدر قلق كبير يجب معالجته قبل نشر RFID في أنظمة الرعاية الصحية. الهدف الرئيسي من هذا المشروع هو تطوير بروتوكول مصادقة RFID أفضل يضمن الأمان. حيث قمنا بتحسين البروتوكول السابق Agrahari et al التي كانت مبنية على ECQV مع خوارزمية جديدة kyber.CPA PKE والتي تعتبر مرشحًا في معايير NIST للتشفير بعد الكم. استخدمنا kyber.CPA PKE الذي يتكون من خوارزمية توليد المفتاح والتشفير وفك التشفير لتحقيق هدفنا والتغلب على نقاط الضعف هذه التي كانت موجودة من قبل. يتم تأكيد أمان مخططنا من خلال التحليلات الأمنية بناءً على العديد من المقاييس. إلى جانب ذلك، فهو متوافق مع علامات RFID منخفضة التكلفة. كما انه يحقق بروتوكولنا أداءً أفضل ويلبي المتطلبات الأساسية. وبالتالي، فإن البروتوكول المقترح قادر على توفير أمان ممتاز لأنظمة الرعاية الصحية القائمة على تقنية تحديد الترددات الراديوية.

الكلمات المفتاحية : المصادقة، نظام الرعاية الصحية، تقنية تحديد الترددات الراديوية، الأمن.

RESUME

La technologie d'identification par radiofréquence (RFID) a été utilisée ces dernières années pour mettre en place des systèmes de santé améliorés, fournissant une variété de services de santé qui peuvent bénéficier à la fois au personnel médical et aux patients. Cependant, étant donné que les systèmes RFID utilisent des voies de communication non sécurisées, la sécurité est une préoccupation majeure qui doit être résolue avant que la RFID puisse être déployée dans les systèmes de santé. L'objectif principal de ce projet est de développer un meilleur protocole d'authentification RFID qui assure la sécurité. Nous avons amélioré un protocole précédent Agrahari et al. Qui était basé sur ECQV avec un nouvel algorithme kyber.CPA PKE considéré comme un candidat dans la normalisation de la cryptographie post-quantique du NIST. Nous avons utilisé kyber.CPA PKE qui consiste en un algorithme de génération de clé, de cryptage et de décryptage pour atteindre notre objectif et surmonter ces faiblesses qui existaient auparavant. La sécurité de notre système est confirmée par des analyses de sécurité basées sur plusieurs mesures. De plus, il est compatible avec les étiquettes RFID à faible coût. De plus, notre protocole atteint de meilleure performance et répond aux exigences de base. Ainsi, Le protocole suggéré est capable de fournir une excellente sécurité pour les systèmes de santé basés sur la RFID.

Mots -clés : Authentification, système de santé, RFID, sécurité.

Summary

List of Figures

List of Tables

General introduction

Radio Frequency Identification is a globally accepted technology, whether we realize it or not, it's a fast pervading wireless data collection technology having radio transmission that contains some identifying information about the objects for automatic identification. In RFID systems, the devices use electromagnetic fields wirelessly to exchange the identifying data. Therefore, RFID has been widely adopted by the healthcare environment for the applications such as infant protection [1], location tracking of medical assets [2], medical treatments tracking and validation [3], patient tracking and medication management [4], blood transfusion, and healthcare management of nursing house.

Since healthcare data is an important part of personal privacy information [5], it is essential to protect the medical private data from being exposed during the processing of RFID authentication. Because is generally exposed to many problems such as information theft, tracking, denial of service. In this case, the privacy and security issues the big problem and it should be highly concerned and taking precautions when healthcare institutions deploy RFID systems.

The main aim of this work is to propose an improved security protocol for RFID authentication in healthcare environment. It is a basic protocol for the traditional backend server based RFID authentication system to ensure the confidentiality and provides mobility, scalability, security, and privacy in the health care environment in a secure communication. We basically look at the pre-existing protocols and see the advantages and disadvantages, take the advantages and try to create a new one that uses these advantages and fills in the disadvantages, we improved [35] by adopting on Kyber.CPA PKE, which is an algorithm safer than others. In order to analyse its security and to evaluate the performance, we use OPENSSL, which consider a software library for applications that secure communications, and for the implementation, we use C as a programming language to compare the computation costs and the communication costs with other protocols that exist before.

Finally, the security of our proposed scheme is analysed against different attacks on RFID, and with the performance of some existing protocols .Then, the research ends with a summary of the results.

Outline:

Chapter 1:

Presentation of the basic terminology of RFID in healthcare , understand its structure, and see the types of existing protocols and the threats to which it was exposed before. Also, the main concepts of security for RFID in healthcare such as security requirement

Chapter 2:

The second chapter, we present the models and related works of authentication scheme using RFID in healthcare.

Chapter 3:

We present a new proposed protocol based on post quantum, where we will ensure more security requirements than the previous scheme.

Chapter 4:

The last chapter contains the performance analysis and security evaluation of our proposed protocol compared to the previous protocols.

CHAPTER 01

RFID IN HEALTHCARE SYSTEMS

1-Introduction

This chapter starts by defining the RFID technology in healthcare and all the main components such as tags, readers and their communication. Then, a general description about the challenges and issues facing the deployment of RFID in healthcare.

2-Definition of RFID:

Radio frequency identification (RFID) is one of the critical technologies of IoT [6]. RFID is a short-range wireless communication technology using radio swells, which can give contactless and automatic object identification [7]. Have the eventuality to increase the trust ability of information, and dramatically change the capability to gain real- time information on the position and parcels of tagged people or objects [8].

3-RFID components:

In a RFID system, there are three components: backend server, RFID reader and RFID tag.

- **RFID tag:** RFID tags, also known as transponders, are identification devices that are attached to objects. Each tag typically consists of an antenna constructed from a small coil of wires; a microchip used to store information electronically about the object (e.g. a vehicle or a container); and encapsulating material to enclose the chip and the coil. Like there are various types of barcode, RFID tags are available with different memory sizes and encoding options. However, an RFID tag offers the capability to store a unique serial number and product information for each item, not just the class of the items. The tag can also incorporate sensors to record temperature, shock, or humidity, for example, providing the ability to track and report on an object's environmental characteristics dynamically.

  The tags may be classified into two main types namely; passive and active tags. Passive RFID tags do not have their own power supply and they take required energy from the radio waves generated by RFID reader. On the other hand, active RFID tags are equipped with their own power source (battery) [9]. RFID tags have simple on-tag circuit and communication protocols; this is why passive tags are prone to cloning, spoofing, relay, replay, eavesdropping, and DoS attacks.

- **RFID reader:** An RFID reader, also called an interrogator or scanner, is the device used to communicate with the RFID tag. It emits RF signals to, and receives radio waves from, the tag via an antenna or antennas. The reader converts the received radio

Waves into digital information that is usually passed to a backend system. Readers, either as stationary or handheld devices, consist of a transmitter, receiver, antenna, microprocessor, controller, memory and power source.

- **RFID backend server:** A backend system, sometimes referred to as an online database, is needed to collect, filter, process, and manage the RFID data. The backend stores complete records of product information, tracking logs, and key management information associated with the RFID tags.

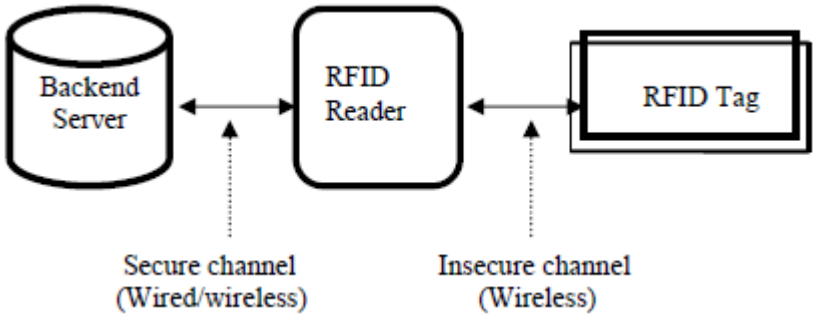


Figure 1.1: Interaction between tag, reader, and backend server. [10]

.

4-RFID characteristics:

Object identification, monitoring, alarm generating, and authentication are all required features of any RFID system. RFID tags have a unique ID and can read data automatically. RFID tags do not need to be in direct line of sight to communicate; they can communicate through insulating materials. From a distance of several meters, hundreds of tags can be scanned every second and are durable and reusable; this tag has a limited storage capacity, a silicon microprocessor for logical processes, and a wireless communication antenna.

These characteristics of RFID tags make them the best option to be used in a several domains; Accordingly, RFID has perceptible benefits, such as reducing cost and time, mitigating human resources, preventing possible theft, and improving productivity [11].

5-RFID in healthcare:

RFID technology have been applied in the healthcare system due to their abilities to aid in identifying, tracking, and validation of staff, equipment, and processes and to provide all sorts of services, such as for the location tracking of medical assets [12], new born and patient identification [13], medical treatments tracking and validation [3], patient location and procedure management at a wellness centre [14], and surgical process management [15]. Figure 1.2 shows a RFID based healthcare system. The users of this system include doctors, nurses and patients. In the system, tags are attached to some objects such drugs, medical assets and patients themselves.

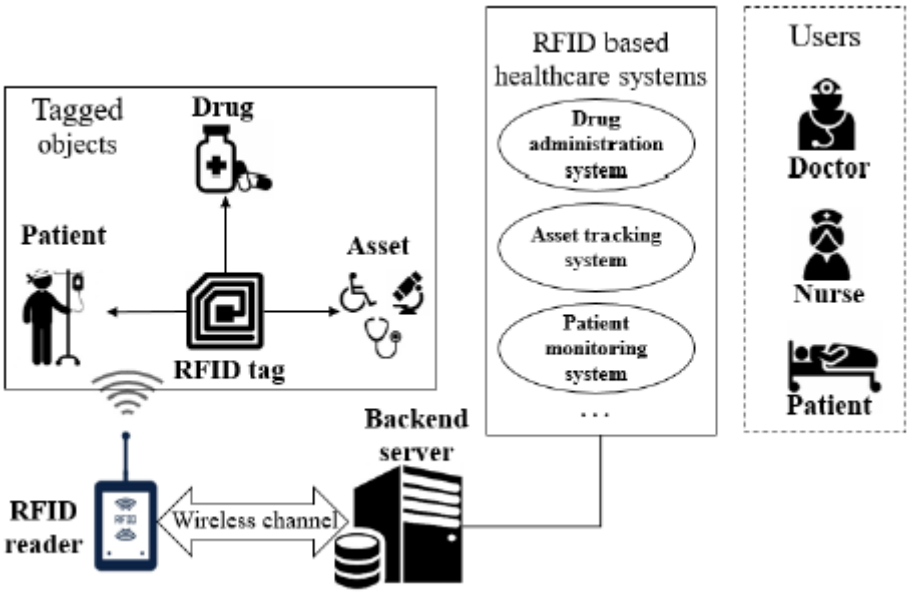


Figure 1.2: RFID based healthcare system. [16]

Through tracking, management, and validation, radio-frequency identification (RFID) technology has the potential to improve patient safety. Furthermore, RFID can ease communication between medical personnel and patients, reducing the time spent waiting for care.

RFID readers can be used by nurses to check the integrity and availability of medications. It is also possible to trace the position of medical assets. As a result, with RFID aid, drug and medical asset management can be greatly enhanced. A patient's tag (embedded in a wearable device or implanted in the body) typically includes some personal information about the patient, such as name, age, and insurance information, which can be used for identification. Medical personnel can also track the tag to rapidly locate the patient. This type of patient

surveillance is extremely beneficial to for the elderly or disoriented patients, and children [17]. More importantly, the tag can collect the patient's physical health data. With a RFID reader, a nurse can collect the data from the tag, and then communicate with the backend server so that the doctors, who are authorized by the patient, can access the patient's physical health data remotely, which achieves remote patient monitoring.

6- Security requirements in RFID based healthcare system:

New security and privacy vulnerabilities exist in an RFID-based healthcare system, which is cause for concern [18]. Because hospitals are considered open environments, and because the tag-to-reader and reader-to-server communication channels in the system are wireless, the tags used in the applications are at risk of being read or duplicated by unauthorized users [19]. The majority of RFID systems now in use are based on ISO 15693, which lacks suitable security features to assure data confidentiality and integrity [12].

6.1 RFID Attacks:

Attacks against an RFID system can be divided into four categories: attacks on authenticity, attacks on integrity (data forgery [19]), attacks on confidentiality, and attacks on availability. In addition to being subject to conventional attacks like tag tracing, eavesdropping, man-in-the-middle attacks, and denial of service. This part shows some types of attacks:

- **Eavesdropping:** Since an RFID tag is a wireless device that emits data, usually a unique identifier, when interrogated by an RFID reader, there exists a risk that the communication between tag and reader can be eavesdropped. Eavesdropping occurs when an attacker intercepts data with a compliant reader—one for the correct tag family and frequency—while a tag is being read by an authorized RFID reader. Since most RFID systems use clear text communication, due to tag memory capacity or cost, eavesdropping is a simple but efficient means for the attacker to obtain information on the collected tag data. The information picked up during the attack can have serious implications—it can be used in subsequent attacks against the RFID system.
- **Man-in-the-middle attack:** While data is in transit from one component to another, An attacker can disrupt the communication line between RFID components and modify the information passed back and forth. This is a threat that is occurring right now. The attack exposes the information before it reaches the intended device and has the ability to alter it in route [44]. Even if it received some inaccurate data, the system being attacked may mistakenly believe the problem is due to network faults and fail to notice the attack.

Because RFID tags are small and inexpensive, they are particularly vulnerable to MITM attacks. This means that there is a general lack of advanced security protection circuitry.

- **Denial of Service (DoS):** DoS attacks can target the RFID tag, the network, or the backend, among other things. The goal is to disable the RFID system so that it cannot be used, not to steal or manipulate information. Physical layer attacks, such as jamming and interference, are the primary issue when discussing DoS attacks on wireless networks. Noise jamming in the RFID system's frequency band can impair network throughput and disrupt network connectivity, resulting in overall supply chain failure. Jamming occurs when a device that actively emits radio signals is able to obstruct and impair the operation of all RFID readers in the vicinity. Interference with other radio transmitters can also be used to launch a denial-of-service attack, obstructing communication between the tags and the reader. Another kind of DoS is to remove RFID tags from things, wash out their contents completely, or wrap them in metal foil to disable or destroy them.
- **Tracking:** Unlike the RFID attacks previously outlined, tracking is a threat directed at a single person. Many more household products may be equipped with item-level RFID tags in the coming years. There is a privacy risk because RFID technology can be used to follow people's travels and even generate a precise profile of their purchases, rather than tracking books and consumer products like apparel.

6.2 RFID Security and privacy:

The healthcare domain is complicated, and while the adoption of a new technology requires sophisticated planning in order to preserve the security and privacy of patient data ,to provide countermeasures against these attacks in many cases specially the issues of confidentiality, unforgeability, location privacy, as discussed below [20, 21]:

- **Confidentiality:** The enormous economic, psychological, and social harm that individuals can incur when personal health information is disclosed necessitates ensuring the privacy of information obtained during health-care activities. As a result, the messages sent through such a system must be encrypted to ensure that no private information is revealed, such as the patient's ID number or health status.
- **Unforgeability:** It is vital to preserve the integrity of health-care data by ensuring that it cannot be altered without authorization. This implies neither the tag nor the reader can be imitated or fabricated.

- **Privacy of the location:** In order to preserve patients' privacy, the RFID system must be able to protect data relating to their treatment and whereabouts. An unauthorized individual should not be able to track a tag or find out where it has been in the past. As a result, the system should be built in such a way that no one outside the system can relate the output to a specific tag.

This section illustrates different kinds to provide countermeasures against attacks that previously mentioned:

- Establishing a secure channel and/or encrypting the communication between tag and reader are two ways to prevent eavesdropping. Another option is to merely include enough information in the tag to identify the object.
- Encrypting communications, transferring information over a secure channel, and providing an authentication mechanism are all technologies that can be used to mitigate MITM threats.
- In general, it's easier to identify DoS assaults than it is to prevent them. Once detected, however, the attacks may usually be stopped before they cause too much damage. Countermeasures against jamming can, for example, use passive listening to detect tags whose transmission exceeds a loudness, and then use block functions to prevent them from transmitting. Enhancing the mechanical connection between the tags and the products, or adding an alarm function to active tags, could be used as a deterrent to disconnecting the tags from the targeted items.
- An easy method to disable tracking is to deactivate the RFID tags, which is known as “killing” the tag that will be introduced in the following section.

From pervious, it is clear that authentication and encryption are the most important security techniques for the protection of RFID based healthcare system .We can use them to address a wide variety of security threats.

6.3 Cryptographic primitives:

The security of RFID systems is primarily concerned with data security and mutual authentication between tag–reader and reader–back-end database server.

- **Hash function:**

A hash function takes two or more characters as input and converts them to a hash value or hash code that is shorter than the input. To put it another way, a hash value, often known as

a hash code, is a fixed-size fingerprint of a variable-size input. A good and effective hash function should have a high level of collision resistance, which implies that no two inputs should produce the same hash code or hash value at the output.

Traditional hash functions such as SHA-1, SHA-2, and MD5 consume many resources to operate. Devices with limited resources necessitate lightweight hash-based solutions, and these lightweight hash-based RFID solutions can be classified into a single category. In an RFID system, any of the Hash functions in this class can be used to accomplish mutual authentication, data privacy, location privacy (un-traceability), and other goals. [22, 23].

Object identifying information is transferred across a wireless channel between RFID tags and a back-end database server, according to the authors of [24], therefore privacy and validity of the transmitted data is of prime importance. For this purpose, mutual authentication among the RFID tags and the back-end database system is indispensable.

- **Secret Key Cryptography:**

Secret Key Cryptography, or symmetric cryptography, uses a single key to encrypt data. Both encryption and decryption in symmetric cryptography use the same key, making this the easiest form of cryptography. The cryptographic algorithm utilizes the key in a cipher to encrypt the data, and when the data must be accessed again, a person entrusted with the secret key can decrypt the data. Secret Key Cryptography can be used on both in-transit and at-rest data, but is commonly only used on at-rest data, as sending the secret to the recipient of the message can lead to compromise. Examples:

- AES: Advanced Encryption Standard (AES) is a symmetric, also known as secret key; ciphers use the same key for encrypting and decrypting. The sender and the receiver must both know -- and use -- the same secret key.
- DES: Data encryption standard (DES) is a common standard for data encryption and a form of secret key cryptography (SKC), which uses only one key for encryption and decryption. Public key cryptography (PKC) uses two keys.
- Caesar Cipher: is one of the simplest and most well-known encryption techniques.

- **Public Key Cryptography:**

Public Key Cryptography, or asymmetric cryptography, uses two keys to encrypt data. One is used for encryption, while the other key can decrypt the message. Unlike symmetric cryptography, if one key is used to encrypt, that same key cannot decrypt the message, rather the other key shall be used.

One key is kept private, and is called the "private key", while the other is shared publicly and can be used by anyone, hence it is known as the "public key". The mathematical relation of the keys is such that the private key cannot be derived from the public key, but the public key can be derived from the private. The private key should not be distributed and should remain with the owner only. The public key can be given to any other entity. Example:

- ECC: Elliptic Curve Cryptography is a key-based technique for encrypting data. ECC focuses on pairs of public and private keys for decryption and encryption of web traffic.
- Diffie-Hellman: A method used to securely exchange or establish secret keys across an insecure network.
- DSS: Digital Signature Standard (DSS) is a digital signature algorithm developed by the U.S. National Security Agency as a means of authentication for electronic documents.

7- Conclusion:

RFID seems to be promising in the method in which health care services are provided to patients with cutting edge technology. In this chapter we have presented general concepts of RFID system, his components and characteristics, we have seen the RFID in healthcare and his structure, also we have discussed about the security problems we see the most attacks on the RFID system , As a result, we see some solutions to achieve security and privacy in RFID . We understand the mechanisms of authentication using RFID based healthcare system. In the next chapter, we will focus on the related works to make the comparison.

CHAPTER 02

RELATED WORKS

1-Introduction:

In this chapter, we review some previous related works that have done, and then we give the pros and cons of each work individually.

2- Authentication protocol for RFID based healthcare system:

Authentication is a primary method for ensuring RFID security. Authentication is a process of confirming the identity claimed by an entity. In the context of a tamper-resistant authentication protocol for an RFID system, the tag and reader establish a trusted relationship and agree on a common, secret, session key to secure the communication between them.

3- Classes of authentication protocols:

According to Chien [25] authentication, protocols are classified into four groups based on the tag's computing cost and supported operations:

- Fully fledged protocols: Protocols that support symmetric and asymmetric encryption, and a one-way function. Examples are in [26, 27].
- Simple protocols: Protocols that support hash function and random number generator (RNG). Examples of this class are given in [28, 29].
- Lightweight protocols: Protocols that support cyclic redundancy check (CRC) and RNG. Examples are given in [30–31].
- Ultra-lightweight protocols: Protocols that are tailored specially to extremely constrained devices. These protocols involve only simple bitwise operations (like AND, OR, XOR) on tags. Examples are given in [32, 33].

In our work, we interest by asymmetric-key and hash based authentication schemes.

4-Cryptographic-based protocols:

In recent years, many authentication protocols have been suggested. Among them, some are based on symmetric key cryptography and some on asymmetric based cryptography. While some are lightweight protocols, others are hash based [34]. Table 2.1 shows the comparison between the protocols.

4.1 Agrahari et al. [35]:

This work presented a secure authentication protocol for RFID, which is based on the concept of an implicit certificate. They used Elliptic curve Qu-Vanstone (ECQV), one kind of implicit certificate. The authors aimed to provide a protocol that fulfils mobility, scalability, security,

and privacy requirements, Moreover; it gives low costs based on the small key size and low computations that the elliptic curve Qu-Vanstone offers compared to traditional elliptic curves.

4.2 Xie et al. [36]:

This work presented two solutions for RFID authentication in healthcare environment. The first one is a basic protocol for the traditional backend server based RFID authentication system to reduce costs,. The second one is an extension protocol for the cloud computing primarily based scenario. They implements the techniques of indistinguishability obfuscation (Io), symmetric encryption, and puncturable pseudo random function. Moreover, their protocols are scalable and practical. [36] Achieved most of the security a requirements of RFID authentication system.

4.3 Zhu et al. [37]:

This work showed a secure mutual authentication protocol (SecMAP) based on hash and squaring root solving operations as crypto-primitives. They implemented quadratic residues theorem to confirm the validity of both the reader and the tag to help server compute information's to the reader. [37] Have a security level higher than others.

4.4 Safkhani et al. [38]:

In this work, they proposed an improved protocol. The main idea is involving all protocol parties in the randomizing of the transferred messages. In addition, the only reliable source for the time could be the server. Hence, the server in the protocol introduces the timestamp and it will verify the round trip time validity. Their protocol's security is also done both informally and formally through the Scyther tool.

4.5 Benssalah et al. [39]:

In in this work, the [39] based on using ECC and elliptic curve digital signature with message recovery to encrypt data transferred between the reader and the server. Moreover, the internet links all of the entities together. Because [39] represented an extended and improved IoT-based RFID authentication scheme for WBANs.

4.6 Gabsi et al. [40]:

In [40], they presented a novel secure ECC-based RFID authentication protocol. Their scheme provides confidentiality, anonymity, forward security properties, and resistance against impersonation and position tracking attacks.

4.7 Kumar et al. [41]:

In this work [41] they proposed an enhanced ECC based lightweight protocol for RFID systems. Their lightweight protocol is more secure and performance efficient than the existing RFID

protocols, and is well suited for practical applications. Their scheme provides the forward Security and backward Security.

5-Comparaison of related works:

Table 2.1 present the comparison between the existing and studied RFID authentication schemes.

Table 2.1: Comparison of various existing RFID authentication schemes

Scheme	Methodology	Verificated by	strengths	weaknesses
Agrahari et al. [35]	ECC based cryptography	AVISPA	The scheme provides mobility, scalability, security, confidentiality and privacy.	Insecure against forward secrecy nor backward secrecy.
Xie et al. [36]	symmetric encryption + puncturable pseudo random function + indistinguishability obfuscation	-	The scheme avoids sensitive data leakage in the server	The scheme are not competitive in efficiency. The scheme does not take advantage of any security simulation tool such as Scythes, AVISPA, and CryptoVerif..
Zhu et al. [37]	Hashed based cryptography + quadratic residues	the Gong-Needham-Yahalom (GNY) logic and the Scyther tool	The scheme provide the resistance to desynchronization attacks The scheme ensures Untraceability, Resilience to replay attacks, Forward secrecy and Mutual authentication..	The communication and the computation cost of SecMAP is high.
Safkhani et al. [38]	Hashed based cryptography	Scyther Tools	Resistance against all kinds of impersonation attack and replay attacks	Insecure against Forward secrecy , no scalability

Benssalah et al. [39]	ECC based cryptography + ECDS	Randon oracle model	The scheme provide Mutual Authentication, Scalability, and Availability. The scheme is well suitable for low-cost RFID systems.	The scheme does not take advantage of any security simulation tool such as Scyther, AVISPA, and CryptoVerif. Does not provide forward Security, tag untraceability and anonymity properties, opposing they claimed.

6- Conclusion:

In this chapter, we have compared between various schemes and we have seen how it work, we have presented the strengths and weaknesses of each one. As a result, we see the difference between the cryptographic primitive like ECC, Hash function. In the next chapter, we will focus on suggesting an improved protocol that achieves more security than the previous one using a new algorithm.

CHAPTER 03

PROPOSED PROTOCOL

1- Introduction:

In this chapter, we will present an improvement to a protocol found in the previous chapter by developing and adopting it on post quantum cryptography , which this kind of encryption consider as more secure because it can resist several common attacks, in the same time the quantum attacks. Moreover, it ensures the least time. As a result, using post quantum cryptography in the design of authentication protocols is required to ensure healthcare applications security.

2- Post-quantum :

The post-quantum schemes that are currently in the NIST competition are either key encapsulation mechanisms (KEMs) or signatures and they can be classified into the following categories :

- **Hash-based cryptography** comprises of hash-based signatures that rely only on certain properties of the underlying hash functions like second-preimage resistance. In round 2 of the NIST competition there are only 2 hash-based signatures: SPHINCS and Picnic. To be noted that Picnic is not only based on hash functions, but it requires a zero-knowledge proof system based on hash functions and block ciphers. However out of these 5 categories, it _ts best in the hash-based cryptography.
- **Code-based cryptography** is based on the hardness of decoding a code word with random errors. In the NIST competition there are currently 7 code-based schemes, all of them KEMs. For example, one of them is Classic McEliece which is a representative scheme in the field as it is based on the first code-based scheme which uses Goppa codes
- **Multivariate cryptography** is based on the hardness of solving systems of quadratic equations in many variables. In the NIST competition there are currently 4 multivariate-based schemes, all of them signature schemes .
- **Isogeny-based cryptography** is based on the hardness of finding bisogenies (mappings) between elliptic curves over finite fields. There is only one KEM scheme currently in the NIST competition, namely SIKE8.
- **Lattice-based cryptography** includes KEMs and signature schemes based on NTRU and on the Learning With Errors (LWE) problem.

In this desseration we will focus on Kyber, a module-LWE-based key-encapsulation mechanism. The main reason for chosing Kyber algorithm is Kyber provides different post-quantum security levels which enables a fair comparison with the NewHope algorithm.

3- Kyber algorithm:

Kyber PKE is a candidate in NIST post-quantum cryptography standardization consisting of key generation, encryption and decryption algorithms. It is considered an IND-CCA2-secure key-encapsulation mechanism (KEM), the security of Kyber is based on the hardness of solving the learning-with-errors problem in module lattices (MLWE problem). The construction of Kyber follows a two-stage approach: we first introduce an INDCPA-secure public-key encryption scheme encrypting messages of a fixed length of 32 bytes, which we call Kyber.CPAPKE. We then use a slightly tweaked Fujisaki–Okamoto (FO) transform to construct the IND CCA2-secure KEM. [42]

Principle of Kyber.CPAPKE algorithm:

A Public Key Encryption scheme (PKE) consists of three probabilistic algorithms (KeyGen, Enc, and Dec).

1. KeyGen () (Key Generation) is an algorithm that outputs a key pair (PK; SK) where PK is the public key and SK is the corresponding private key.

2. Enc (PK) (Encryption) is a probabilistic algorithm that takes a public key PK and a message m and produces a cipher text C.

3. Dec(SK; C) (Decryption) is a deterministic algorithm that takes as input a secret key SK and a cipher text C and return a message m , or in case of rejection, the symbol ?.

Kyber.CPAPKE is parameterized by integer's n, k, q, η 1, η 2, du, and dv, throughout Kyber512 parameter sets: n = 256, k =2, q = 3329.

Moreover, we given **A** as a global polymatrix with coefficients sampled from uniform distribution in NTT domain, a simplified version is shown as follows:

• **Kyber. KeyGen (A):** Choose two polyvec **s**, **e** from $\beta_\eta{}^k$ and compute **t** = **As** + **e**. The public key is (**A**, **t**) and the private key is **s**.

• **Kyber. Enc (A.t.m):** The sender encodes the message m to polynomial m' with an encoder designed to tolerate introduced errors by mapping ''0'' bits to 0 and ''1'' bits to $\lceil q/2 \rfloor$. Sample polyvec **r** from $B\eta_1$, **e1** and ***e*2** from $B\eta_2$. The cipher text then consists of polyvec **u** = $\mathbf{A}^T$ **r** + **e**1 and polynomial v = $\mathbf{t}^T$ **r** + $e2$ + m.

• **Kyber. Dec (s.u.v):** The recipient computes $m' = v - \mathbf{s}^T$ **u** and recover the original message m from polynomial m' using a decoder. The decoder is used to decode a coefficient to ''1'' bit if the coefficient of m' is closer to $\lceil q/2 \rfloor$ than to 0, and decode to a ''0'' bit otherwise.

Generally speaking, $'$ is not equal to m, because the error polyvec $\mathbf{e}1$ and error polynomial $e2$ are introduced in the encryption process. If the private key is correct, the decrypted m is equal to the original plaintext with a negligible probability of decryption failure, because the encoder and decoder can tolerate the errors.

Table 3.1: List of notations.

Symbol	Meaning
SK	Secret key
PK	Public key
S	Server
||	Concatenation of two inputs
ID_T	I' the Tag identifier
PK_T	I' the Tag public key
SK_T	I 'the Tag secret key
PK_S	Server public key
SK_S	Server secret key
SID	I' Session identifier
η	Noise of s and e
CPA	Chosen Plaintext Attack
CBD	Centred binomial distribution
PRf	PseudoRandom function
T	Timestamps
h( )	One-way hash function
s,e	two polyvec from β_η^k
r	Random coins
$\oplus$	XOR operation
PKE	Public Key Encryption
NTT	Number Theoretic Transform
CCA	Adaptive Chosen Ciphertext Attack
NIST	National Institute of Standards and Technology
IND	Indistinguishable
LWE	Learning With Errors
ECDS	Elliptic Curve Digital Signature
IOT	Internet of things
ISA	Instruction Set Architecture

4- The proposed protocol:

In the proposed protocol, we assume the communication channel between reader and backend server is fully secure. In addition, we assume that our server is trusted Authority (TA). The proposed protocol is divided into two phases, the registration phase, and the authentication phase. The summary of these phases is given in Fig 3.1.

4.1 Registration phase:

This phase consists of two steps:

We have secret key SK and public key PK; and we use hash function and CPA.KYBER function to encrypt and decrypt the messages.

Step1. When the Tag T wants to register with the server S, the tag choose an identification ID_T and sends it to the server.

Step2. After receiving the registration request, S generate a matrix A[i][j] and calculates the public key PK and secret key SK of tag .and stores them in database, and takes them back to the tag. And loads {ID_T, PK_T, SK_T, SID} into its memory.

4.2 Authentication phase:

The mutual authentication phase consists of the following steps:

Step1. When a Tag T wants to interact with the server S, the tag generates a timestamp T1 and calculates a hash message H1= h (ID_T || T1) || ID_T and encrypts message C= CPA. ENC (ID_T || T1), and sends them to the server.

Step2. Server receiving the messages H1 and the message C from encryption algorithm

CPA.Enc, it decrypts the message C with his secret key SK_S.

Step3. After the reception of message H1 and message C, the server verify if timestamp T is valid. If ID_T found in database, the server generate T2; the server authenticates the tag and calculates message H1'=h (SID || T2 || SID), If H1= H1' the tag is verified. After it computes new messages Z= CPA. ENC $_{PKT}$ (SID || T2) and a hash message E=h (SID || T2) $\oplus$ T1. Then, it sends Z, E, and T2 to the tag T.

Step4. After the tag receive of messages Z and E from decryption algorithm CPA.Dec; it verifies if timestamp T2 is valid, and calculates message Z1= h (ID_T || T2) $\oplus$ T2.

Then, it verify Z=Z1 if yes the server is valid.

Step5. Finally, the tag calculates the shared session key SK and in the other side, the server

Computes the same session key SK=h (SID || T2 || T1).

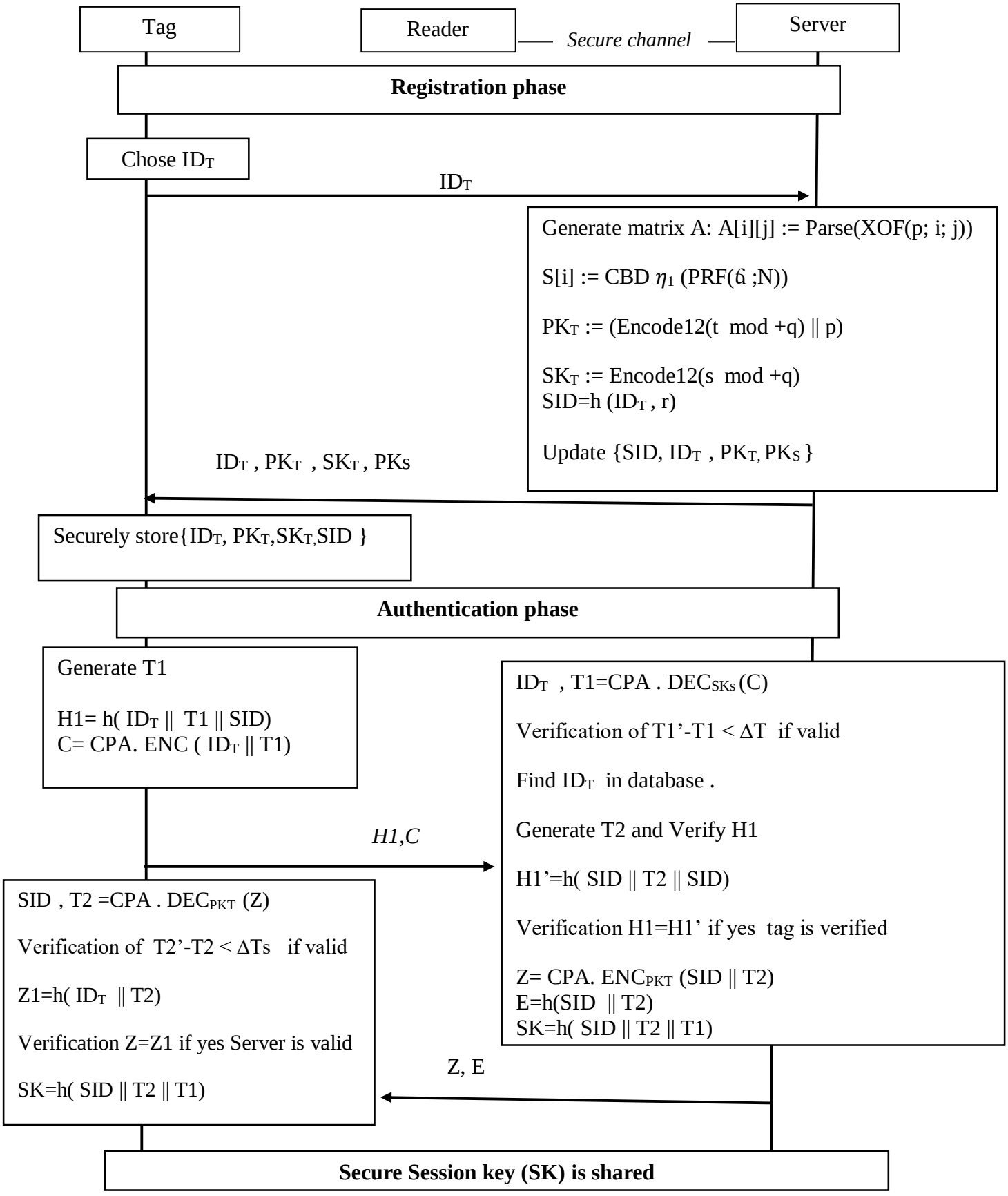


Figure 2.1: Illustration of proposed authentication protocol

5- Conclusion:

This chapter present the phases of our proposed scheme, as shown we chose Kyber.CPAPKE an encryption algorithm for protecting .and the phases it went through to share the session Key SK. The next chapter we will see the implementation, analyse the security requirements and evaluate the performance.

CHAPTER 04

PERFORMANCE ANALYSIS AND SECURITY EVALUATION

1. Introduction:

In this chapter we review the performance analysis and security evaluation of the proposed protocol that we discus in pervious chapter .Reeling on several criteria to compare our scheme with the previously schemes mentioned and to ensure its effectiveness.

2. Security analysis:

Security analysis is a crucial part of any scheme. This section demonstrates that our proposed protocol is secure against many well-known attacks. Security is a significant concern in the healthcare environment as patient life is involved. In this section, we discuss the security and privacy requirements of our proposed scheme by using: informal analysis .Table 4.1 summarizes a security comparison between our scheme and previous schemes.

- **Mutual authentication:**

Mutual authentication means both the legitimate tag and the server should authenticate each other. Especially when they need to communicate in an insecure channel. Here, the tag and the server communicate in the insecure channel. In the improved protocol, S firstly verifies the validity of ID_T. After that, S authenticates T by checking whether H1=H1'. On the other hand, T authenticates S by verifying whether Z=Z1 and compute a valid session key SK. After S receives C, it can verify the equality C= Z to authenticate ID_T and to establish the session key SK. Therefore, our improved protocol ensures mutual authentication.

- **Confidentiality:**

In health-care, the data is sensitive and must be protected in an insecure data transmission channel. The information between the tag and server is shared as the identifier ID_T, timestamps T, public key PK, secret key SK. To protect them, we used: an encryption algorithm CPA.Enc which resists indistinguishability under adaptive chosen-cipher text attack , a robust cryptographic hash function .Moreover , the intruder cannot obtain any secret data ,because we use a secure cryptographic primitives and they are not sent clearly over the insecure channel. Hence, our proposed protocol provides confidentiality.

- **Forward secrecy:**

The tag stores data (ID_T, PK_T, SK_T, SID) in its memory. At the end of each session, the value of T is updated by the new value, which is shared with the server. The adversary cannot acquire the last timestamps T used in the previous sessions, and he cannot confirm whether the message came from tag or server. Thus, the proposed protocol achieves forward secrecy.

- **MITM attack:**

The attacker cannot obtain the secret data and the session key because all secret data are encrypted by public-key encryption scheme CPA.Enc and protected by a secure cryptographic hash function. However, the session key is generated at the end of the protocol and not transmitted in the communication channel. We suppose that the attacker is of type active, and then, it can modify the exchanged messages when the attacker modifies the values of the transmitted messages C, H, Z, E, by different values C', H1',Z', E'. Consequently, the authentication will be unsuccessful. Therefore, our protocol is secure against the MITM attack and the attacker cannot cheat the legal entities.

- **Anonymity and traceability attack:**

Tag Anonymity means that the adversary should know the tag and tag identifier's location if the tag response message is constant. However, here in our scheme we use authentication protocol, which mean we have a high level to protect the privacy .Moreover, Id_T is well protected by using encryption algorithm CPA.Enc, and a secure hash function. With these different mechanisms of protection, the attacker cannot obtain the secret identifier Id_T of tag. Therefore, the proposed scheme ensures device anonymity and protects devices against traceability attack.

- **Session key establishment:**

The session key SK computed in end of authentication protocol is used to encrypt the secret information during send messages between the tag and server. SK is a symmetric key for one unique use and is changed in each session of communication. In our scheme Tag and server calculate the session key SK=h (SID || T2 || T1).

Table 4.1: Security comparison.

Protocol\ Requirement	D1	D2	D3	D4	D5	D6	D7
Agrahari et al. [35]	**Y**	**N**	**N**	**Y**	**–**	**–**	**N**
Xie et al. [36]	**Y**	**Y**	**–**	**N**	**Y**	**Y**	**N**
Zhu et al. [37]	**Y**	**Y**	**Y**	**Y**	**–**	**–**	**N**
Safkhani et al. [38]	**Y**	**Y**	**N**	**Y**	**–**	**N**	**N**
Benssalah et al. [39]	**N**	**Y**	**–**	**N**	**Y**	**Y**	**N**
Our Protocol	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**

D1: Mutual Authentication; **D2:** confidentiality**; D3:** Forward secrecy;
D4: Anonymity and traceability attack; **D5:** MITM; **D6:** Session key establishment
D7: Quantum attack
"Y": the requirement is achieved.
"N": the requirement is not achieved.
"–": the requirement is not discussed

- **Post quantum:**

In the previous schemes, no one measures security against quantum attack, because they used primitive encryption algorithms such as ECC. But in our scheme we use encryption algorithms based on LWE IND-CPA secure key-encapsulation mechanism (KEM), which is more protective against several common attacks.

3. Performance evaluation:

The computation capability and communication cost of the tags are very limited as compared to the reader and the backend server in an RFID system. Therefore it is essential that besides security and privacy. For thus we evaluate the computational and communication cost of the proposed protocol and compare it with the studied in the previous protocols.

3.1 Implementation:

We compare the computational and communication costs of the proposed protocol to those of the some protocols studied [35, 39]. We override of the computational cost of CPA.Kyber encryption/decryption operations by using its library [42]. In addition, we use library openssl to override the hash function, and ECC scalar multiplication. For the measurements, we used a PC on Kali Linux of processor x64 Intel (R) Celeron (R) CPU 1000M @ 1.80GHz memory 3.89 Go. In our proposed protocol, we agreed the parameters of Kyber.CPAPKE code with the

security level of 128 bits. In CPA.KYBER based protocols, we take 768 bytes of cipher text and 32 bytes of Encryption message in our evaluation.

In our work, we use SHA-512, ECC-512 and Kyber.CPAPKE-512 to standardize the size of all values in terms of cost both of time and of communication. Moreover, because random numbers are generated using a hash function, random number generation times are estimated to be equal to SHA-512 execution times. We assumed that the concatenation, xor operation are ignored in terms of running time.

Table 4.2 present the performance of implementation of cryptographic primitives in our machine.

Table 4.2: Performance of implementation of cryptographic primitives in PCS.

Symbol	Description	Timing (ms)
T_h	Execution time of hash operation	0.011
T_{Enc}	Execution time of encryption operation in the proposed CPA scheme	0.1
T_{Dec}	Execution time of decryption operation in the proposed CPA scheme	0.036
T_M	Execution time of scalar point multiplication in ECC	4.226
T_A	Execution time of addition operation in ECC	0.704

Table 4.3: Comparison in computational cost

Scheme	Tag side computational cost	Server side computational cost	Total computational cost	Total in milliseconds
Agrahari et al. [35]	$5T_{MUL} + T_A + T_h$	$6\ T_{MUL} + T_A + T_h$	$11T_{MUL} + 2\ T_A + 2T_h$	47.916
Safkhani et al. [38]	$2T_h + R$	$4T_h + R$	$6T_h + 2R$	0.088
Benssalah et al. [39]	$2T_{MUL} + 3T_h$	$T_{MUL} + 3T_h$	$3\ T_{MUL} + 6\ T_h$	12.744
Our proposed Protocol	$3T_h + T_{ENC} + T_{DEC}$	$4T_h + T_{ENC} + T_{DEC}$	$7T_h + 2T_{ENC} + 2T_{DEC}$	0.349

T_h: Time to compute hash operation; **T_{ENC}:** Kyber encryption operation;

T_{DEC}: Kyber decryption operation; **T_{MUL}:** Time to compute scalar multiplication operation;

T_A: Time to compute addition operation; **R:** random number generator (operation).

3.2 Computational cost:

The results of execution time of cryptographic primitives RFID components are shown in Table 4.2. These results show that scalar multiplication is more than 42 times expensive than encryption operation of the proposed scheme and more than 117 times expensive than the decryption operation.

Table 4.3 shows that our proposed protocol computational cost is less than other existing protocols. Thus, our protocol achieves better performance and it fulfils the basic requirements, which were necessary to create a secure and authentic healthcare system. These results show that the value of the computational cost of Agrahari et al. [35] and [39] are 47.919 ms and 12.744 ms, respectively.

In the proposed scheme, there is no utilization of ECC, Pseudo-Kasami code Kc because all these operations usually require high computational resources. Instead, we have utilized Kyber.CPAPKE encryption/decryption operations, SHA-512, in our proposed scheme which needs less execution time 0.349 ms. The analysis shows that our scheme is preferable for low-cost tags for RFID systems as illustrated in Fig. 4.1.

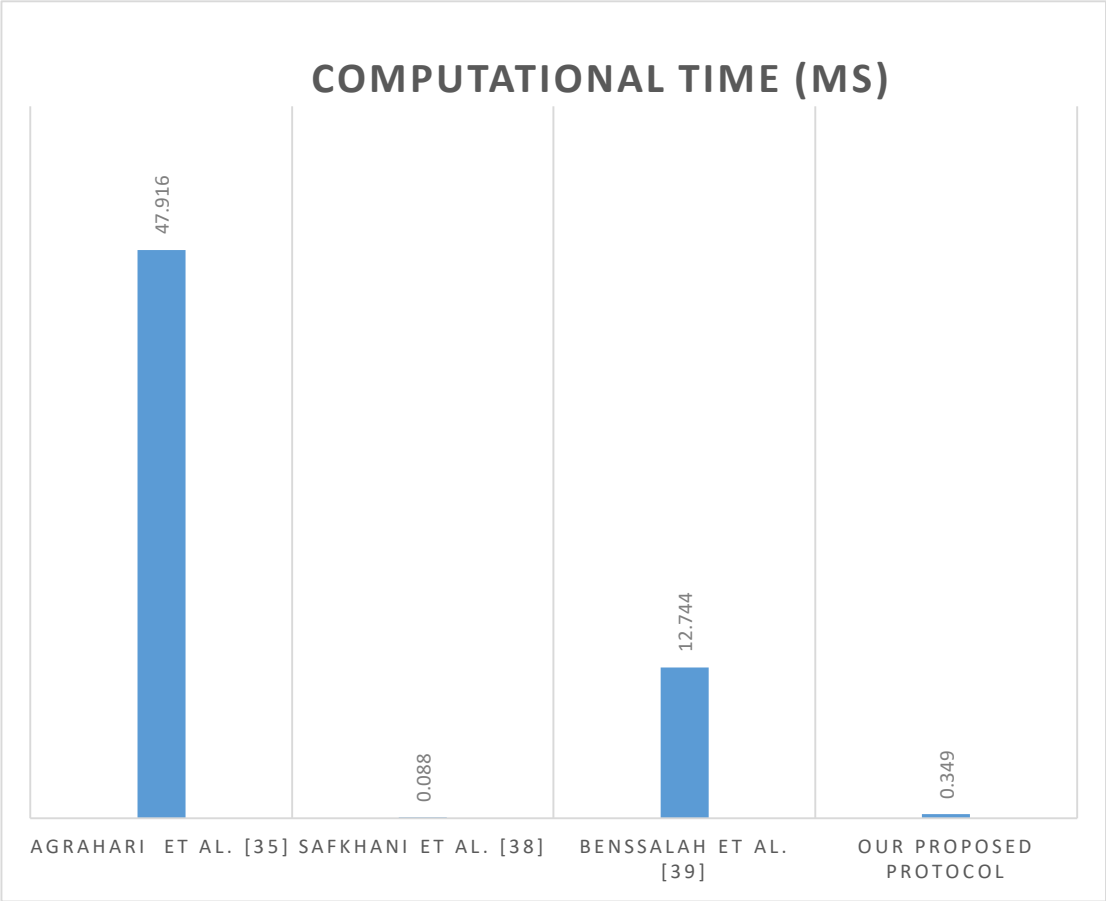


Figure 3.1: Comparison of computational time (MS).

3.3 Communication cost:

Table 4.4 presents the communication cost of our proposed protocol and other studied protocols. The tag transmits the total number of messages in one authentication session run. In our scheme, the communication cost is more than those of other protocols not based on post quantum. It can be justified because our scheme offers better security than all other protocols. The graphical comparison of the proposed scheme for the communication costs between other schemes in Fig 4.2. Overall, the proposed protocol is not outstanding at communication cost.

Table 4.4: Communication cost comparison.

Protocol	Communication cost (Bytes)
Agrahari et al. [35]	288
Safkhani et al. [38]	576
Benssalah et al. [39]	288
Our proposed Protocol	768*2 + 32*2= 1600

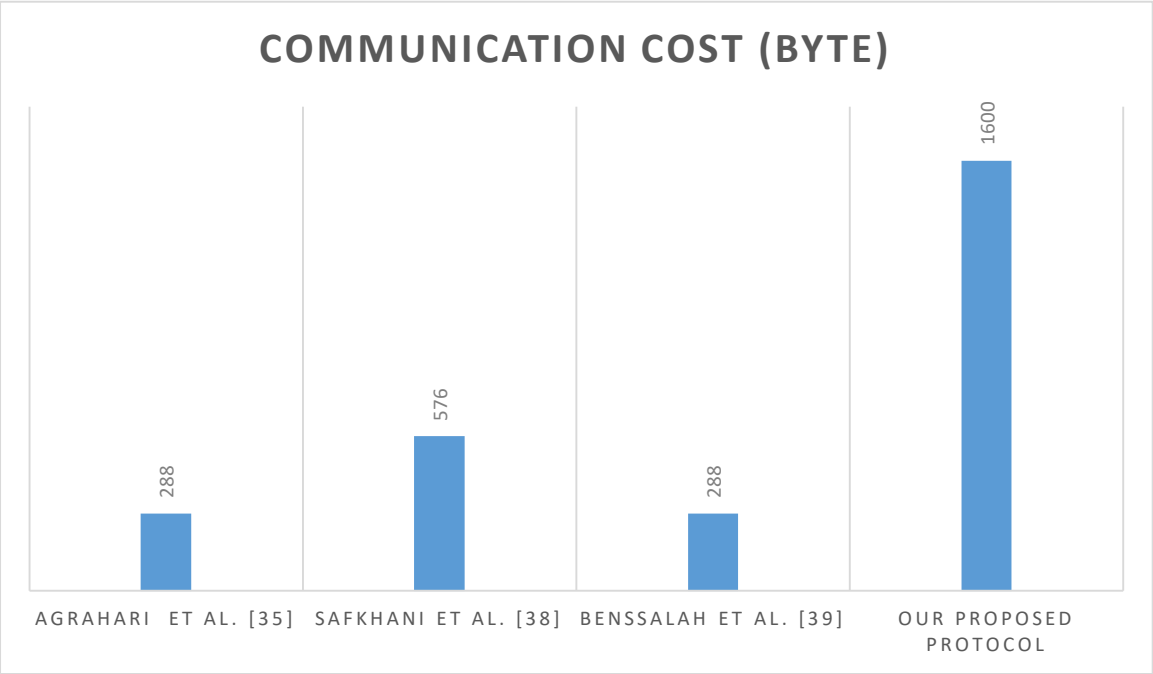


Figure 4.2: Total number of communication.

4. Conclusion:

In this chapter, we implemented the security analysis based on several criteria and we compare it with the previous schemes that exist. Moreover, we evaluated the performance (The computation capability and communication cost) of each protocol. The result shows that our scheme achieved better performance and it fulfils the basic requirements which were necessary to create a secure and authentic healthcare system.

General Conclusion

RFID authentication protocols have gained much popularity due to extensive use of RFID in the healthcare domain, due the patient data is more sensitive, because it contains personal information, medical history, physical examination, medication use history, immunization status, and even some sound and visual data. We have first focused on RFID security and privacy in this study by encrypting and hashing their data files to allow fine-grained access, giving him ultimate control over their privacy by using CPAPKE-Kyber algorithm. Thus, ensure the impressive efficiency and the strong security level, which we do not find in most existing protocols .Furthermore, an efficiently evaluated improved protocol has been proposed in the work that offers reduced calculation overhead and interesting security performance. In our work, we have analysed the effectiveness of our proposed protocol against Mutual Authentication, confidentiality, Forward secrecy, Anonymity and traceability attack, MITM session key establishment and Quantum attack. A comparative study between our protocol and existing work has shown its effectiveness in terms of ensured security and computing performance. Our proposed protocol presents a good compromise between its calculation performance and its strength against different attacks.

For future work, we will continue to improve our work by implementing AVISPA tool to check its security effectiveness formal. Moreover, our scheme will be implemented of authentication protocol in RFID tags.

Bibliography:

[1] Wyld, D. C. (2010). Preventing the "worst case scenario:" combating the lost laptop epidemic with RFID technology. In Novel algorithms and techniques in telecommunications and networking (pp. 29-33). Springer, Dordrecht.

[2] Wang, S. W., Chen, W. H., Ong, C. S., Liu, L., & Chuang, Y. W. (2006, January). RFID application in hospitals: a case study on a demonstration RFID project in a Taiwan hospital. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) (Vol. 8, pp. 184a-184a). IEEE.

[3] Katz, J. E., & Rice, R. E. (2009). Public views of mobile medical devices and services: A US national survey of consumer sentiments towards RFID healthcare technology. International journal of medical informatics, 78(2), 104-114.

[4] Martínez Pérez, M., Cabrero-Canosa, M., Vizoso Hermida, J., Carrajo García, L., Llamas Gómez, D., Vázquez González, G., & Martín Herranz, I. (2012). Application of RFID technology in patient tracking and medication traceability in emergency care. Journal of medical systems, 36(6), 3983-3993.

[5] Fan, K., Jiang, W., Li, H., & Yang, Y. (2018). Lightweight RFID protocol for medical privacy protection in IoT. IEEE Transactions on Industrial Informatics, 14(4), 1656-1665.

[6] Fan, K., Gong, Y., Liang, C., Li, H., & Yang, Y. (2016). Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. Security and Communication Networks, 9(16), 3095-3104.

[7] Juels, A. (2006). RFID security and privacy: A research survey. IEEE journal on selected areas in communications, 24(2), 381-394.

[8] Wang, S. W., Chen, W. H., Ong, C. S., Liu, L., & Chuang, Y. W. (2006, January). RFID application in hospitals: a case study on a demonstration RFID project in a Taiwan hospital. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) (Vol. 8, pp. 184a-184a). IEEE.

[9] Yousuf, Y., & Potdar, V. (2008, March). A survey of RFID authentication protocols. In 22nd International Conference on Advanced Information Networking and Applications-Workshops (aina workshops 2008) (pp. 1346-1350). IEEE.

[10] Dass, P., & Om, H. (2016). A secure authentication scheme for RFID systems. Procedia Computer Science, 78, 100-106.

[11] Ajami, S., & Rajabzadeh, A. (2013). Radio Frequency Identification (RFID) technology and patient safety. Journal of research in medical sciences: the official journal of Isfahan University of Medical Sciences, 18(9), 809.

[12] Najera, P., Lopez, J., & Roman, R. (2011). Real-time location and inpatient care systems based on passive RFID. Journal of Network and Computer Applications, 34(3), 980-989.

[13] Hung, Y. K. (2007). The study of adopting RFID technology in medical institute with the perspectives of cost benefit. In International Medical Informatics Symposium in Taiwan, Taiwan.

[14] Leu, J. G. (2010). The benefit analysis of RFID use in the health management center—the experience in Shin Kong Wu Ho-Su Memorial Hospital. National Taiwan University.

[15] Yu, C., Chen, C., Liao, P., & Lee, Y. (2008). RFID-based operation room and medicare system for patient safety enhancement—a case study of keelung branch. J. Inf. Manag, 15, 97-122.

[16] Zhu, F. (2020). SecMAP: a secure RFID mutual authentication protocol for healthcare systems. IEEE Access, 8, 192192-192205.

[17] Haddara, M., & Staaby, A. (2018). RFID applications and adoptions in healthcare: a review on patient safety. Procedia computer science, 138, 80-88.

[18] Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications, 153, 311-335.

[19] Hwang, M. S., Wei, C. H., & Lee, C. Y. (2009). Privacy and security requirements for RFID applications. Journal of Computers, 20(3), 55-60.

[20] Barrows Jr, R. C., & Clayton, P. D. (1996). Privacy, confidentiality, and electronic medical records. Journal of the American medical informatics association, 3(2), 139-148.

[21] Loomis, G. A., Ries, J. S., Saywell, R. M., & Thakker, N. R. (2002). If electronic medical records are so great, why aren't family physicians using them?. Journal of Family Practice, 51(7), 636-641.

[22] Yang, L., Yu, P., Bailing, W., Yun, Q., Xuefeng, B., & Xinling, Y. (2013). Hash-based RFID mutual authentication protocol. International Journal of Security and Its Applications, 7(3), 183-194.

[23] Dehkordi, M. H., & Farzaneh, Y. (2014). Improvement of the hash-based RFID mutual authentication protocol. Wireless personal communications, 75(1), 219-232.

[24] Li, Y., & Teraoka, F. (2012, September). Privacy protection for low-cost RFID tags in IoT systems. In Proceedings of the 7th International Conference on Future Internet Technologies (pp. 60-65).

[25] Chien, H. Y. (2007). SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. IEEE transactions on dependable and secure computing, 4(4), 337-340.

[26] Tuyls, P., & Batina, L. (2006, February). RFID-tags for anti-counterfeiting. In Cryptographers' track at the RSA conference (pp. 115-131). Springer, Berlin, Heidelberg.

[27] Feldhofer, M., Dominikus, S., & Wolkerstorfer, J. (2004, August). Strong authentication for RFID systems using the AES algorithm. In International workshop on cryptographic hardware and embedded systems (pp. 357-370). Springer, Berlin, Heidelberg.

[28] Tsudik, G. (2006, March). YA-TRAP: Yet another trivial RFID authentication protocol. In Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06) (pp. 4-pp). IEEE.

[29] Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2004). Security and privacy aspects of low-cost radio frequency identification systems. In Security in pervasive computing (pp. 201-212). Springer, Berlin, Heidelberg.

[30] Bringer, J., Chabanne, H., & Dottax, E. (2006, June). HB^+^+: a lightweight authentication protocol secure against some attacks. In Second international workshop on security, privacy and trust in pervasive and ubiquitous computing (SecPerU'06) (pp. 28-33). IEEE.

[31] Gilbert, Henri, Matthew Robshaw, and Herve Sibert. "Active attack against HB/sup+: a provably secure lightweight authentication protocol." Electronics letters 41.21 (2005): 1169-1170.

[32] Li, T., & Deng, R. (2007, April). Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol. In The Second International Conference on Availability, Reliability and Security (ARES'07) (pp. 238-245). IEEE.

[33] Li, T., & Wang, G. (2007, May). Security analysis of two ultra-lightweight RFID authentication protocols. In IFIP international information security conference (pp. 109-120). Springer, Boston, MA.

[34] Chien, H. Y. (2009). The study of RFID authentication protocols and security of some popular RFID tags. Development and implementation of rfid technology, 261-291.

[35] Agrahari, A. K., & Varma, S. (2021). A provably secure RFID authentication protocol based on ECQV for the medical internet of things. Peer-to-Peer Networking and Applications, 14(3), 1277-1289.

[36] Xie, S., Zhang, F., & Cheng, R. (2021). Security enhanced RFID authentication protocols for healthcare environment. Wireless Personal Communications, 117(1), 71-86.

[37] Zhu, F. (2020). SecMAP: a secure RFID mutual authentication protocol for healthcare systems. IEEE Access, 8, 192192-192205.

[38] Safkhani, M., & Vasilakos, A. (2019). A new secure authentication protocol for telecare medicine information system and smart campus. IEEE Access, 7, 23514-23526.

[39] Benssalah, M., Sarah, I., & Drouiche, K. (2021). An efficient RFID authentication scheme based on elliptic curve cryptography for Internet of Things. Wireless Personal Communications, 117(3), 2513-2539.

[40] Gabsi, S., Kortli, Y., Beroulle, V., Kieffer, Y., Alasiry, A., & Hamdi, B. (2021). Novel ECC-based RFID mutual authentication protocol for emerging IoT applications. IEEE Access, 9, 130895-130913.

[41] Kumar, S., Banka, H., Kaushik, B., & Sharma, S. (2021). A review and analysis of secure and lightweight ECC-based RFID authentication protocol for Internet of Vehicles. Transactions on Emerging Telecommunications Technologies, 32(11), e4354.

[42] crystals, https://pq-crystals.org/kyber/ access :22/05/2022

[43] Liu, Z., Wenger, E., & Großschädl, J. (2014, June). MoTE-ECC: Energy-scalable elliptic curve cryptography for wireless sensor networks. In *International Conference on Applied Cryptography and Network Security* (pp. 361-379). Springer, Cham.

[44] Welch, D., & Lathrop, S. (2003, June). Wireless security threat taxonomy. In IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003. (pp. 76-83). IEEE.

.