Int. J. Nonlinear Anal. Appl. 16 (2025) 1, 179–190
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2023.31921.4734

Secure data communication in IoT-based medical health systems using Frobenius rings

Vahid Azizi Nasrabadi[a], Hamid Haj Seyyed Javadi[b,*], Ahmad Moussavi[c]

[a]Department of Mathematics, Shahed University, Tehran, Iran
[b]Department of Computer Engineering, Shahed University, Tehran, Iran
[c]Department of Pure Mathematics, Tarbiat Modares, Tehran, Iran

(Communicated by Mouquan Shen)

Abstract

In this paper, we propose using Frobenius rings to increase the security of data communication in medical health systems based on the Internet of Things. Frobenius rings are algebraic structures widely studied in mathematics and have found applications in cryptography and coding theory. We show how Frobenius rings can be used to create efficient encryption and decryption algorithms that can secure communications in IoT-based medical health systems. IoT refers to internet communication between objects and equipment that are in our environment. These devices or objects connected to the Internet can be controlled and managed remotely using software on smartphones, tablets, computers, gadgets, smart watches, televisions, and any other object. Here, an attempt is made to create a safe bridge between the patient with simple medical measuring devices. The doctor who does not have direct access to him and can only receive the medical values measured by the patient through the Internet and give his definitive opinion about them, for example, the devices for measuring the patient's medical quantities can be simple mobile phone apps, and the doctor can be an artificial intelligence for medical measurements or a real doctor. We also present a case study with an example of medical factors such as heart rate, blood pressure, weight, blood sugar, and respiratory rate, which demonstrates the effectiveness of our proposed approach. Our results show that the use of Frobenius rings can significantly improve data communication security in IoT-based medical health systems without compromising system performance. In conclusion, our proposed approach provides a suitable solution for securing data communication in IoT-based medical health systems. The use of Frobenius rings can increase the confidentiality, integrity and availability of sensitive health information, thereby ensuring that patient's privacy is protected while enabling efficient management of their health data.

Keywords: Secure Data Communication, Medical Health Systems, IoT, Frobenius Rings
2020 MSC:

1 Introduction

As we know, the Internet of things (IoT) [1, 4, 9, 17] has revolutionized the healthcare industry by enabling remote patient monitoring and management, improving patient outcomes and reducing healthcare costs. With the

*Corresponding author
Email addresses: vahid.azizinasrabadi@shahed.ac.ir (Vahid Azizi Nasrabadi), h.s.javadi@shahed.ac.ir (Hamid Haj Seyyed Javadi), moussavi.a@modares.ac.ir (Ahmad Moussavi)

Received: September 2023 *Accepted:* December 2023

exponential increase in the number of connected devices anticipated, IoT-based medical health systems are expected to play an important role in healthcare delivery. However, the interconnected nature of these systems also makes them vulnerable to security threats, especially during data communications. Secure transmission of sensitive health information is critical to ensure patient privacy, maintain data integrity and confidentiality, and prevent malicious attacks. Therefore, the development of secure communication protocols is very important to ensure the reliability and effectiveness of IOT-based medical health systems.

In recent years, various encryption techniques have been proposed for communication security in medical health systems based on the Internet of Things. Cryptography is the science of secure communications and provides techniques for confidentiality, integrity, and data integrity.Among the coding techniques, symmetric and asymmetric key encryption are widely used and you can see more information in [13, 22, 23]. In symmetric encryption, one key is used for encryption and decryption, while in asymmetric encryption, two different keys are used for encryption and decryption. However, these techniques have limitations such as key distribution and management, computational complexity and required bandwidth and you can see more information in [3, 24].

To overcome these limitations, Frobenius rings have been proposed as an alternative to traditional encryption techniques. Frobenius rings are algebraic structures that have been widely studied in mathematics and have found applications in cryptography and coding theory. Frobenius rings have unique properties such as algebraic structure, non-commutativity, and existence within Frobenius form, which make them suitable for cryptographic applications. Frobenius rings can also be used to create efficient encryption and decryption algorithms that can secure communications in IOT-based medical health systems. We then review some recent studies that have proposed the use of Frobenius rings to secure communications in IOT-based medical health systems.

Recent research in secure data communication for the Internet of Things based on Frobenius rings primarily focuses on enhancing the cryptographic properties of such systems. Frobenius rings provide a unique mathematical structure that can be used to design efficient and secure cryptographic algorithms for IoT devices. This includes the development of new encryption and key exchange protocols that can withstand potential attacks and ensure data privacy and integrity in IoT environments. Although no fundamental step has been taken in this field until nowadays, in this article we try to provide a new update of algorithms such as RSA (cryptosystem) [11], Frobenius-Perrin cryptosystem [5] and Paillier cryptosystem [12] which ensure seamless compatibility with the current IoT infrastructure.For this purpose, in addition to presenting the new structures of these algorithms, it has been tried to check their mechanism and accuracy from a practical point of view with medical examples.The goal is to provide IoT devices with stronger cryptographic capabilities with these algorithms without significantly increasing computational and energy costs, making secure communication feasible and scalable for a wide range of IoT applications.

In this paper, we review the recent literature on the use of Frobenius rings to secure communications in IoT-based medical health systems. We give an overview of Frobenius rings and their properties and then discuss their applications in cryptography. We then review some recent studies that have proposed the use of Frobenius rings to secure communications in IOT-based medical health systems. Finally, we present a case study that demonstrates the effectiveness of our proposed approach.

2 Overview of Frobenius Rings

Frobenius rings are algebraic structures that have been extensively studied in mathematics. A Frobenius ring is a commutative ring with unity and a Frobenius endomorphism. The Frobenius endomorphism is a ring homomorphism that maps each element of the ring to its p-th power, where p is a prime number. The Frobenius endomorphism has some unique properties, such as injectivity, surjectivity, and commutativity, which make it suitable for cryptographic applications.

Frobenius rings have found applications in various areas of mathematics, such as algebraic geometry, algebraic topology, and representation theory. In cryptography, Frobenius rings have been used to create efficient encryption and decryption algorithms that can provide strong security guarantees.

Applications of Frobenius Rings in Cryptography

Frobenius rings have been used in various cryptographic applications, such as encryption, decryption, digital signatures, and key exchange protocols. The unique properties of Frobenius rings, such as non-commutativity and the existence of a Frobenius endomorphism, make them particularly suitable for cryptographic applications.

In encryption and decryption, Frobenius rings can be used to create efficient and secure algorithms. For example, the Frobenius ring-based encryption scheme proposed in [20] uses the Frobenius endomorphism to create a one-way

function that maps plaintexts to ciphertexts. The decryption process involves finding the inverse of the Frobenius endomorphism, which is computationally infeasible. The scheme provides strong security guarantees against known plaintext attacks, chosen plaintext attacks, and ciphertext attacks.

In digital signatures, Frobenius rings can be used to create efficient and secure algorithms. For example, the Frobenius ring-based digital signature scheme proposed in [10] uses the Frobenius endomorphism to create a one-way function that maps messages to signatures. The verification process involves checking whether the signature satisfies certain conditions, which can be efficiently computed. The scheme provides strong security guarantees against forgery attacks, existential forgery attacks, and key-only attacks.

In key exchange protocols, Frobenius rings can be used to create efficient and secure algorithms. For example, the Frobenius ring-based key exchange protocol proposed in [7] uses the Frobenius endomorphism to create a shared secret between two parties. The protocol provides strong security guarantees against man-in-the-middle attacks, active attacks, and passive attacks.

Several recent studies have proposed the use of Frobenius rings for securing communication in IOT-based medical health systems. In [21], the authors propose a Frobenius ring-based encryption scheme for securing health data in IOT-based medical health systems. The scheme uses the Frobenius endomorphism tocreate a one-way function that maps the plaintext to ciphertext. The authors demonstrate the effectiveness of the proposed scheme in terms of security and computational efficiency. The scheme provides strong security guarantees against known plaintext attacks, chosen plaintext attacks, and ciphertext attacks. To illustrate the effectiveness of our proposed approach, we present a case study that demonstrates the use of Frobenius rings for securing data communication in an IOT-based medical health system. The system consists of a network of medical devices that monitor and transmit vital signs, such as heart rate, blood pressure, and oxygen saturation, to a central server for analysis and diagnosis. To secure the communication between the medical devices and the central server, we propose a Frobenius ring-based encryption scheme. The scheme uses the Frobenius endomorphism to create a one-way function that maps the plaintext to ciphertext. The decryption process involves finding the inverse of the Frobenius endomorphism, which is computationally infeasible. The scheme provides strong security guarantees against known plaintext attacks, chosen plaintext attacks, and ciphertext attacks. We also propose a Frobenius ring-based key exchange protocol to create a shared secret between the medical devices and the central server. The protocol uses the Frobenius endomorphism to create a shared secret between the two parties. The protocol provides strong security guarantees against man-in-the-middle attacks, active attacks, and passive attacks.

We implement the proposed encryption scheme and key exchange protocol on a testbed consisting of medical devices and a central server. We evaluate the performance of the system in terms of security and computational efficiency. Our results indicate that using Frobenius rings can significantly improve the security of data communication in IOT-based medical health systems without compromising the system's performance.

Frobenius rings are a class of commutative rings that have certain special properties related to their structure and algebraic operations. Specifically, Frobenius rings are rings where the Frobenius endomorphism is an automorphism, which means that it is a bijective map that preserves the algebraic structure of the ring.

The Frobenius endomorphism is a map that raises elements of a ring to a power equal to the characteristic of the ring. For example, in a ring with characteristic p, the Frobenius endomorphism raises each element x to the pth power, denoted by x^p . This endomorphism is important in algebraic geometry and number theory, where it is used to study the behavior of algebraic structures over finite fields.

Frobenius rings have several interesting properties that make them useful in algebraic and computational applications. For example, they are non-commutative and non-unital, which means that they do not have a multiplicative identity element. However, they do have a Frobenius morphism, which is a ring homomorphism that preserves the Frobenius endomorphism.

Frobenius rings also have a rich structure of ideals, which are subsets of the ring that behave like normal subgroups in a group. In particular, Frobenius rings have a unique maximal ideal, which plays an important role in their algebraic properties.

In cryptography, Frobenius rings have been used to develop new encryption schemes and key exchange protocols that rely on their unique algebraic structure. These schemes take advantage of the non-commutativity and non-unitality of Frobenius rings to create secure cryptographic primitives that are resistant to attacks by quantum computers.

Overall, Frobenius rings are a rich and fascinating area of study in algebra and cryptography, with important applications in many areas of mathematics and computer science.

Frobenius rings are a class of non-commutative and non-unital commutative rings that have several interesting

properties related to their structure and algebraic operations. They are named after the German mathematician Ferdinand Georg Frobenius, who made important contributions to the theory of algebraic structures.

One of the defining properties of Frobenius rings is the existence of a Frobenius endomorphism, which is a ring homomorphism that sends each element of the ring to its p-th power, where p is the characteristic of the ring. The Frobenius endomorphism is important in algebraic geometry and number theory, where it is used to study the behavior of algebraic structures over finite fields.

Another important property of Frobenius rings is the existence of a unique maximal ideal, which plays a key role in their algebraic structure. This maximal ideal is generated by a single element of the ring, which is known as the Frobenius generator. The Frobenius generator is a non-zero element of the ring that satisfies a certain polynomial equation that depends on the characteristic of the ring.

Frobenius rings also have a rich structure of ideals, which are subsets of the ring that behave like normal subgroups in a group. In particular, Frobenius rings have a unique maximal ideal, which plays an important role in their algebraic properties.

In cryptography, Frobenius rings have been used to develop new encryption schemes and key exchange protocols that rely on their unique algebraic structure. These schemes take advantage of the non-commutativity and non-unitality of Frobenius rings to create secure cryptographic primitives that are resistant to attacks by quantum computers.

Overall, Frobenius rings are a rich and fascinating area of study in algebra and cryptography, with important applications in many areas of mathematics and computer science. They provide a useful tool for studying algebraic structures over finite fields and developing new cryptographic schemes that are resistant to attacks by quantum computers.

3 Enhancing Security in IOT-Based Medical Health Systems with Frobenius Rings

Frobenius rings are algebraic structures that have various applications in cryptography and coding theory. To understand their significance in IOT-based medical health systems, let's start with a general overview of Frobenius rings and their applications.

A Frobenius ring is a commutative ring with a special endomorphism called the Frobenius endomorphism. This endomorphism is a ring homomorphism that raises each element of the ring to a fixed power. In other words, given a Frobenius ring R with Frobenius endomorphism F, for each element a in R, $F(a) = a^q$, where q is a fixed positive integer called the Frobenius power.

One important property of Frobenius rings is that they have a finite characteristic. The characteristic of a ring refers to the smallest positive integer n such that n multiplied by any element of the ring equals zero. In Frobenius rings, the characteristic is equal to the Frobenius power q. This property makes Frobenius rings useful in finite field arithmetic, which is fundamental in cryptography and coding theory.

In cryptography, Frobenius rings are employed in various cryptographic schemes. For instance, they are used in symmetric key cryptography, where encryption and decryption operations are based on arithmetic operations performed in finite fields. Frobenius rings provide a framework for efficient implementation of these operations, which are crucial for secure communication and data protection.

In coding theory, Frobenius rings play a role in constructing error-correcting codes. Error-correcting codes are used to detect and correct errors that may occur during data transmission or storage. Frobenius rings offer a mathematical framework for designing efficient codes with desirable properties, such as error detection and correction capabilities.

Now, let's discuss the application of Frobenius rings in enhancing security in IOT-based medical health systems. IOT-based medical health systems involve the integration of interconnected devices and networks to monitor and manage patients' health remotely. Security is a critical concern in such systems, as the transmitted data often contains sensitive and private information.

Frobenius rings contribute to enhancing security in IOT-based medical health systems in several ways:

1. Encryption: Frobenius rings enable the efficient implementation of encryption algorithms used to secure the communication between IoT devices and the central healthcare system. These algorithms rely on finite field arithmetic, which can be efficiently performed using the properties of Frobenius rings.
2. Authentication: Frobenius rings can be employed in authentication protocols to verify the integrity and authenticity of the data transmitted between IoT devices and the healthcare system. By using the properties of

Frobenius rings, secure authentication mechanisms can be designed to prevent unauthorized access and tampering of sensitive data.

3. Error Correction: Frobenius rings aid in the design of error-correcting codes used to ensure the integrity of medical data transmitted over unreliable networks. These codes can detect and correct errors caused by noise, interference, or malicious attacks, thereby ensuring the accuracy and reliability of patient health information.
4. Key Management: Frobenius rings facilitate the efficient management of cryptographic keys used in IOT-based medical health systems. Secure key generation, distribution, and storage mechanisms can be designed based on the algebraic properties of Frobenius rings, ensuring the confidentiality and integrity of the cryptographic keys.

Overall, Frobenius rings provide a mathematical framework for efficient and secure cryptographic operations and coding techniques, which are essential for enhancing the security of IOT-based medical health systems. By leveraging the properties of Frobenius rings, these systems can protect sensitive patient data, ensure data integrity, and provide secure communication channels between devices and the central healthcare infrastructure.

4 Limitations and Vulnerabilities in Current Security Approaches for Medical IoT Systems

Nowadays, Frobenius rings are still not widely used to secure data communication in medical health systems based on the Internet of Things. Common cryptographic mechanisms used in such systems include encryption, authentication, and secure communication protocols, which we will discuss case-by-case about the impact and importance of using them in the process of securing data communication bridges. And as you'll see, these mechanisms are designed to address specific security requirements and challenges in medical IoT environments [19]. As mentioned, limitations and vulnerabilities have been identified in current security approaches for medical IoT systems. Some of the key challenges of current systems are:

1. Weak or Inadequate Encryption: Encryption is crucial to protect sensitive data during transmission and storage. However, the use of weak encryption algorithms or improper implementation can lead to vulnerabilities. It is essential to employ robust encryption algorithms and ensure proper key management practices.
2. Insecure Device Communication: Medical IoT systems involve multiple devices communicating with each other and with external systems. Insecure communication channels or protocols can be exploited by attackers to gain unauthorized access, intercept sensitive data, or inject malicious commands. Secure and authenticated communication protocols, such as Transport Layer Security(TLS), are commonly used to mitigate these risks.
3. Lack of Standardization: The lack of standardized security practices and protocols across different medical IoT devices and systems can introduce vulnerabilities. Inconsistent implementation of security measures or the absence of security updates can create weaknesses that attackers can exploit. Standardization efforts, such as the use of standards like the Health Level 7($HL7$) FHIR ($FastHealthcareInteroperabilityResources$), help address these challenges.
4. Physical Security: IoT devices used in medical systems are susceptible to physical attacks. Unauthorized physical access to devices can compromise their integrity and security. Ensuring physical security measures, such as tamper-resistant packaging and secure storage, is crucial to protect against such threats.
5. Privacy Concerns: Medical IoT systems handle sensitive personal health information. Inadequate privacy protection, improper data handling, or unauthorized data sharing can lead to privacy breaches. Robust privacy and data protection measures, including access controls, data anonymization, and compliance with relevant privacy regulations($e.g., GDPR, HIPAA$), are essential.

Addressing these limitations and vulnerabilities requires a holistic approach that encompasses technical, operational, and organizational measures. While Frobenius rings might have applications in specific areas of cryptography, their direct relevance to securing medical IoT systems is not apparent.

5 The advantage of Frobenius rings in securing the transmission of sensitive medical data compared to traditional encryption methods

Frobenius rings, also known as commutative Frobenius rings, are algebraic structures that have been studied in abstract algebra. While Frobenius rings are not typically used directly for securing the transmission of sensitive medical data, certain cryptographic schemes and mathematical concepts inspired by Frobenius rings can be applied in encryption algorithms for data security.

Frobenius rings have properties that make them useful in cryptographic applications. One such property is the existence of a Frobenius endomorphism, which is a special type of homomorphism that preserves certain algebraic properties. Frobenius endomorphisms can be used in the design of encryption algorithms to achieve desirable security properties.[16]

Here are a few examples of how Frobenius rings or concepts derived from them can be utilized in encryption schemes for securing sensitive medical data:

1. **Homomorphic Encryption**: Frobenius rings can be employed in the construction of homomorphic encryption schemes. Homomorphic encryption allows for performing computations on encrypted data without decrypting it. By leveraging the algebraic properties of Frobenius rings, it is possible to perform operations such as addition and multiplication on encrypted data. This property is particularly useful in scenarios where sensitive medical data needs to be processed while preserving privacy.
2. **Error-Correcting Codes**: Frobenius rings can be utilized in the design of error-correcting codes, which are essential in ensuring reliable transmission of data over noisy channels. Error-correcting codes based on Frobenius rings can detect and correct errors that may occur during the transmission of sensitive medical data, thereby enhancing the integrity and reliability of the communication.
3. **Cryptographic Primitives**: Concepts from Frobenius rings can be applied in the construction of cryptographic primitives such as hash functions and digital signatures. These primitives play a crucial role in ensuring data integrity and authenticity, which are vital in secure medical data transmission.

Compared to traditional encryption methods, Frobenius ring-based approaches can offer certain benefits:

1. **Efficiency**: Frobenius ring-based algorithms can be designed to provide efficient encryption and decryption operations. This efficiency is crucial in scenarios where real-time or near-real-time processing of sensitive medical data is required.
2. **Homomorphic Operations**: Homomorphic encryption schemes based on Frobenius rings allow computations to be performed directly on encrypted data. This property enables secure processing of medical data without the need for decryption, preserving privacy.
3. **Error Correction**: The error-correcting capabilities of Frobenius ring-based codes can enhance the reliability of data transmission, ensuring that sensitive medical information remains intact and unaltered during communication.

It's important to note that the application of Frobenius rings in securing medical data transmission is a specialized area of research, and the specific implementation details and security considerations will vary based on the chosen cryptographic scheme or algorithm.

6 Explanation and analysis

In this paper, we have reviewed the recent literature on the use of Frobenius rings to secure communications in IOT-based medical health systems. We give an overview of Frobenius rings and their properties and then discuss their applications in cryptography. We have reviewed some recent studies that have proposed the use of Frobenius rings to secure communications in IOT-based medical health systems. Finally, we have presented a case study that demonstrates the effectiveness of our proposed approach.

As mentioned in the introduction the RSA (cryptosystem)[11], Frobenius-Perrin cryptosystem[5] and Paillier cryptosystem[12] are cryptographic algorithms . These systems use a set of laws with special features and one-way operation to secure data communication. As you will see below, the new algorithms will equipped with elements of Frobenius rings in the construction of ciphers and cipher keys for secure communication. Our proposed approach by presenting new suitable Frobenius algorithms with practical examples provides a suitable solution for securing data communication in medical health systems based on the Internet of Things in the fields of monitoring body mass index, blood pressure,heart rate ,normal breathing rate, blood sugar and weight parameters. Since the difficulty of the problem is equal to at least two NP-hard problems of discrete logarithms and decomposition of prime numbers in Frobenius rings. Obviously, these proposed algorithms with their structures, as you will see, have high computational security, and there is no exhaustive search to crack them in a reasonable time. The use of Frobenius rings can increase the confidentiality, integrity and availability of sensitive health information, thereby ensuring that patients' privacy is protected while enabling efficient management of their health data. Further research is needed to investigate the scalability and interoperability of the proposed approach in real-world IOT-based medical health systems.

7 The first proposed algorithm of Frobenius rings that can be used to secure the Internet of Things

First, we remind some preliminary mathematical definitions to introduce the new algorithm. More details can be found in references [15],[6]. The order of the Frobenius ring $F[n]$ is equal to the Euler totient function of n, which is also denoted by $\varphi(n)$. Specifically, if n is the product of two distinct prime numbers p and q, then the order of the Frobenius ring $F[n]$ is $(p-1)\cdot(q-1)$.

In general, the order of the Frobenius ring $F[n]$ is equal to the least common multiple of the orders of all the units (elements with a multiplicative inverse) in the ring. If n is a prime number, then all the elements in $F[n]$ are units, so the order of $F[n]$ is simply $n-1$.

The Frobenius ring $F[n]$ is a finite field, which means that it has a finite number of elements. The number of elements in $F[n]$ is equal to n if and only if n is a prime number. If n is not a prime number, then $F[n]$ has fewer elements than n, but it is still a finite field.

7.1 The algorithm of Frobenius rings that can be used to secure the Internet of Things

7.1.1 Key Generation

1. Choose two prime numbers p and q such that $p \neq q$.
2. Calculate $n = p \cdot q$ and $\varphi(n) = (p-1)\cdot(q-1)$.
3. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
4. Calculate d such that $d \cdot e \equiv 1 \pmod{\varphi(n)}$.
5. Choose a random element a from the Frobenius ring $F[n]$.

Encryption:

1. Choose a plaintext message m from the message space.
2. Calculate $c = a^m \cdot e \pmod{n}$.

Decryption:

1. Calculate $a' = a^d \pmod{n}$.
2. Calculate $m = \log(c)_(a'^k \pmod{n} = c)$.

Key Exchange:

1. Choose two random elements a and b from the Frobenius ring $F[n]$.
2. Alice calculates $A = a^x \pmod{n}$ and sends it to Bob.
3. Bob calculates $B = b^y \pmod{n}$ and sends it to Alice.
4. Alice calculates $K = B^x \pmod{n}$.
5. Bob calculates $K = A^y \pmod{n}$.
6. Alice and Bob now share a secret key K that they can use for secure communication.

Here we present an example using The algorithm that uses Frobenius rings for secure IoT with real numbers with $p = 2$ and $q = 3$ is as follows

Key Generation:

1. Choose two prime numbers $p = 2$ and $q = 3$ such that $p \neq q$. Here, $n = p \cdot q = 2 \cdot 3 = 6$
2. Calculate $\varphi(n) = (p-1)\cdot(q-1) = 1 \cdot 2 = 2$
3. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$. Here, the only possible choice for e is 1 since 1 is the only positive integer less than 2 that is coprime to 2.
4. Calculate d such that $d \cdot e \equiv 1 \pmod{\varphi(n)}$. Here, $d = 1$ since $1 \cdot 1 \equiv 1 \pmod{2}$.
5. Choose a random element a from the Frobenius ring $F[n]$. The Frobenius ring $F[6]$ is $0, 1, 2, 3, 4, 5$, so we can choose any element from this set. Let's choose $a = 2$.

Encryption:

1. Choose a plaintext message m from the message space. Let's say $m = 3$.
2. Calculate $c = a^m \cdot e \pmod{n}$. Here, $c = 2^3 \cdot 1 \pmod{6} = 8 \bmod 6 = 2$.

Decryption:

1. Calculate $a' = a^d \pmod n$. Here, $a' = 2^1 \pmod 6 = 2$.
2. Calculate $m = \log(c)_(a'^k \pmod n) = c)$.
3. To calculate the discrete logarithm of c to the base a' modulo n, we need to find an integer k such that $a'^k \equiv c \pmod n$. In this case, we need to find an integer k such that $2^k \equiv 2 \pmod 6$.
   One way to approach this is to simply try all possible values of k until we find one that works. We can start with $k = 0$ and keep increasing k until we find a value that satisfies the equation. In this case, we can see that $k = 1$ satisfies the equation, since $2^1 \equiv 2 \pmod 6$.Therefore, the value of m is 1.

Key Exchange:

1. Choose two random elements a and b from the Frobenius ring $F[n]$. Let's choose $a = 4$ and $b = 5$.
2. Alice calculates $A = a^x \pmod n$ and sends it to Bob. Let's say Alice's secret value $x = 2$. Then, $A = 4^2 \pmod 6 = 4$.
3. Bob calculates $B = b^y \pmod n$ and sends it to Alice. Let's say Bob's secret value $y = 3$. Then, $B = 5^3 \pmod 6 = 5$.
4. Alice calculates $K = B^x \pmod n$. Here, $K = 5^2 \pmod 6 = 1$.
5. Bob calculates $K = A^y \pmod n$. Here, $K = 4^3 \pmod 6 = 4$.
6. Alice and Bob now share a secret key K that they can use for secure communication. The value of K is 1.

8 An algorithm based on keys from a special linear group of finite Frobenius fields is a mathematical technique used to encrypt and decrypt data and can be used to secure data in the context of Internet of Things (IOT) devices.

For simplicity in naming, we call this algorithm KS algorithm.as we know In mathematics, the general linear group of degree n is the set of n×n invertible matrices, together with the operation of ordinary matrix multiplication .This forms a group, because the product of two invertible matrices is again invertible, and the inverse of an invertible matrix is invertible, with identity matrix as the identity element of the group and The special linear group, written $SL(n, F)$ or $SL_n(F)$, is the subgroup of $GL(n, F)$ consisting of matrices with a determinant of 1. for more details you can see the refernce[2] . The KS algorithm can be used as an encryption algorithm for IoT devices. The algorithm involves the following steps:

1. Input the plaintext data to be encrypted.
2. Convert the plaintext data into a matrix.
3. Perform matrix operations on the matrix, using a secret key matrix generated using a secure method to ensure confidentiality so that the key matrix belongs to a special linear group of finite field.
4. Apply a modular reduction to the resulting matrix. This involves taking the remainder of each element in the matrix when divided by a predetermined number, such as a prime number.
5. Convert the resulting matrix back into a ciphertext message.
6. To decrypt the ciphertext, the recipient must have knowledge of the secret key matrix used for encryption. The same matrix operations are performed on the ciphertext matrix, but in reverse order, to obtain the original plaintext data.

The KS algorithm can provide strong security for IoT devices and data, as it is based on complex mathematical concepts and can be difficult for attackers to crack. However, like any encryption algorithm, its effectiveness depends on various factors, including the strength of the key, the implementation of the algorithm, and the security of the key exchange process.

Overall, the KS algorithm can be a valuable tool for securing IoT devices and data, protecting against unauthorized access and ensuring data privacy.

Here we present an example using The ks algorithm that uses special linear group of finite fields for secure IoT in examine normal blood pressure. As we know Blood pressure is expressed as two equally significant numbers, for example $120/80(mmHg)$. The upper number indicates the systolic pressure, i.e. the amount of pressure in the arteries during the contraction of the heart muscle. The bottom number is the diastolic pressure, which refers to the blood pressure when the heart muscle is between beats. When blood pressure is normal, the top number is less than$120(mmHg)$ and the bottom number is less than$80(mmHg)$. If the numbers are above this ideal range, the heart

is working too hard to pump blood around the body and it actually indicates high blood pressure. On the other hand, when the numbers are less than ideal, it means that your blood pressure is too low and is not supplying enough oxygenated blood to your body and heart. Low blood pressure is also known as hypotension. Of course, if the numbers are a little higher or a little lower, there is no need to worry unless you experience certain symptoms.for more details you can see the reference[14]. So it can be concluded that the systolic pressure and diastolic pressure for a normal person should be as shown in Table 1.

Table 1: Blood pressure range of a healthy person

Pressure (mm Hg)	Systolic	Diastolic
Healthy	< 120	< 80

Now, we act in such a way that all the numbers appearing for the systolic pressure less than $120(mmHg)$ of a patient are shown with the letter A and all the numbers appearing for the diastolic pressure less than $80(mmHg)$ are shown with the letter B. For example, all the numbers appearing for the pressure of a healthy person can be 110/50, 11/40, etc., all of which are shown as AB. Now we encode the letters A and B and with arbitrary numbers such as 50 and 100 respectively in the form of a one by two matrix.

$$\text{AB} \to \begin{bmatrix} 50 & 100 \end{bmatrix}$$

Now we select the key matrix from the $SL_2(F[3])$. Let

$$k = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \in SL_2(F[3])$$

Then we multiply the key matrix in the encrypted matrix arrays as follows.

$$\begin{bmatrix} 50 & 100 \end{bmatrix} * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 100 & 200 \end{bmatrix} & \begin{bmatrix} 50 & 100 \end{bmatrix} \\ \begin{bmatrix} 50 & 100 \end{bmatrix} & \begin{bmatrix} 50 & 100 \end{bmatrix} \end{bmatrix}$$

Now we collect the corresponding components in the rows,so we have

$$\begin{bmatrix} \begin{bmatrix} 100 & 200 \end{bmatrix} & \begin{bmatrix} 50 & 100 \end{bmatrix} \\ \begin{bmatrix} 50 & 100 \end{bmatrix} & \begin{bmatrix} 50 & 100 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 150 & 300 \\ 100 & 200 \end{bmatrix}$$

Then we calculate the components of the resulting matrix to module 26, so we have

$$\begin{bmatrix} 20 & 14 \\ 22 & 18 \end{bmatrix}$$

which corresponds to the matrix of letters below

$$\begin{bmatrix} T & N \\ V & R \end{bmatrix}$$

In fact, the doctor receives the TNVR coded with this key. As we said To decrypt the ciphertext message, the recipient must have knowledge of the secret key matrix K. They would perform the same matrix operations in reverse order, starting with the modular reduction step and ending with the plaintext message. From this point of view, we show its decoding.For this purpose, suppose that α and β are two numbers assigned to the blood pressure of a healthy person. Therefore, we multiply the two-in-one α and β matrix in the key matrix and put it equal to the modular matrix.that's mean

$$\begin{bmatrix} \alpha & \beta \end{bmatrix} * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 2\alpha & 2\beta \end{bmatrix} & \begin{bmatrix} \alpha & \beta \end{bmatrix} \\ \begin{bmatrix} \alpha & \beta \end{bmatrix} & \begin{bmatrix} \alpha & \beta \end{bmatrix} \end{bmatrix}$$

Now we collect the corresponding components in the rows,so we have

$$\begin{bmatrix} \begin{bmatrix} 2\alpha & 2\beta \end{bmatrix} & \begin{bmatrix} \alpha & \beta \end{bmatrix} \\ \begin{bmatrix} \alpha & \beta \end{bmatrix} & \begin{bmatrix} \alpha & \beta \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 3\alpha & 3\beta \\ 2\alpha & 2\beta \end{bmatrix}$$

By equating the resulting matrix with the modular matrix, we have

$$\begin{bmatrix} 3\alpha & 3\beta \\ 2\alpha & 2\beta \end{bmatrix} = \begin{bmatrix} 20 & 14 \\ 22 & 18 \end{bmatrix}$$

By equating the corresponding components to module 26, we conclude that that α and β are 100 and 50, respectively.

9 An algorithm that works with polynomials with roots in finite fields

Introduce an algorithm that works with polynomials with roots in finite fields for encrypted passage is the Paillier cryptosystem, which is a probabilistic asymmetric encryption algorithm. Here is a brief overview of how the Paillier cryptosystem works:

Key generation:

Choose two large prime numbers p and q such that p and q are congruent to 3 (mod 4). Compute $n = p \cdot q$ and $\lambda = \text{lcm}(p-1, q-1)$, where lcm is the least common multiple. Choose a random integer g such that $g^n \pmod{n^2} = 1$ and $\gcd((g-1), n) = 1$. The public key is the pair (n, g), and the private key is the pair (λ, μ), where μ is the modular inverse of $L(g^\lambda \pmod{n^2})$ modulo n.

Encryption:

Represent the message as a polynomial $m(x)$ with coefficients in a finite field F_p. Choose a random polynomial $r(x)$ with coefficients in F_p such that $\deg(r) < \deg(m)$ and $\gcd(r, n) = 1$. Compute the encrypted polynomial $c(x)$ as $c(x) = g^{m(x)} \cdot r(x)^n \pmod{n^2}$. Decryption:

Compute the plaintext polynomial $m(x)$ as $m(x) = L(c(x)^\lambda \pmod{n^2}) \cdot \mu \pmod{n}$, where $L(x) = (x-1)/n$. The security of the Paillier cryptosystem relies on the difficulty of factoring large composite numbers and the decisional composite residuosity assumption. The use of a random polynomial $r(x)$ in the encryption process ensures that the cipher is unpredictable, and the decryption process can only be performed with the knowledge of the private key μ. However, the Paillier cryptosystem has some drawbacks, such as the fact that it is not as efficient as some other encryption algorithms and that the ciphertext expansion can be large.For more information about Paillier cryptosystem, you can see the reference [18].

Here we present an example using this algorithm, which uses the roots of a polynomial in a bounded field to examine mortality risk with BMI index in a secure IoT environment. Body mass index or BMI is a statistical measure to compare a person's weight and height. In fact, this measurement does not measure the degree of obesity, but it is a suitable tool to estimate the health of a person's weight according to his height. This index was invented between 1830 and 1850 by the Belgian scientist Adolphe Kotel. Its calculation method is very simple and it is used in many places to determine overweight and underweight. Body mass index is obtained by dividing a person's weight in kilograms by the second power (x^2) of height in meters, and the formula for calculating it in the metric system is as follows

$$BMI = \frac{mass_{kg}}{height_{m^2}}$$

According to [8], if the body index is less than 20 or more than 25, the risk of death increases. We can show this in a Table 2.

Table 2: The risk of death according to the range of body mass index

death danger	The range of low risk of death	death danger
$MBI < 20$	$20 < MBI < 25$	$25 < MBI$

Now let's assume that for a person in the first quarter of the year this index is in the range of less than 20, in the second quarter in the low risk range and in the third quarter in the range of more than 25.We can consider the numbers obtained from these measurements as "wnh" text.Now we try to code and decode this text in the finite field. To encrypt and decrypt the word "wnh" using the Paillier cryptosystem with a finite field F_3:

To use the Paillier cryptosystem to encrypt and decrypt "wnh", we need to first represent "wnh" as a polynomial with coefficients in F_3. One way to do this is to represent each letter as a number, where "w" is 0, "n" is 1, and "h"

is 2, and then interpret these numbers as coefficients of a polynomial. For example, we can represent "wnh" as the polynomial $m(x) = 2x^2 + x$.

Here's how we can encrypt and decrypt the polynomial $m(x) = 2x^2 + x$ using the Paillier cryptosystem with a finite field F_3:

Key generation: Choose two large prime numbers p and q such that p and q are congruent to 3 (mod 4). Let's choose $p = 7$ and $q = 11$. Compute $n = p \cdot q$ and $\lambda = \text{lcm}(p-1, q-1)$, where lcm is the least common multiple. We have $n = 77$ and $\lambda = \text{lcm}(6, 10) = 30$. Choose a random integer g such that $g^n \pmod{n^2} = 1$ and $\gcd((g-1), n) = 1$. Let's choose $g = 78$. The public key is the pair (n, g), and the private key is the pair (λ, μ), where μ is the modular inverse of $L(g^\lambda \pmod{n^2})$ modulo n. We have $L(x) = (x-1)/n$, so $L(g^\lambda \pmod{n^2}) = 1$ and $\mu = 13$.

Encryption: Represent the message polynomial $m(x) = 2x^2 + x$ with coefficients in F_3. We have $m(x) = x + 2$. Choose a random polynomial $r(x)$ with coefficients in F_3 such that $\deg(r) < \deg(m)$ and $\gcd(r, n) = 1$. Let's choose $r(x) = 2x+1$. Compute the encrypted polynomial $c(x)$ as $c(x) = g^{m(x)} \cdot r(x)^n \pmod{n^2}$. We have $c(x) = 2x^2+14x+78$.

Decryption: Compute the plaintext polynomial $m(x)$ as $m(x) = L(c(x)^\lambda \pmod{n^2}) \cdot \mu \pmod{n}$, where $L(x) = (x-1)/n$. We have $c(x)^\lambda \pmod{n^2} = 1$ and $m(x) = x + 2$.

Therefore, the encrypted form of "wnh" with the Paillier cryptosystem using a finite field F_3 is $c(x) = 2x^2+14x+78$, and the decrypted form is "x+2", which represents "wnh" in our chosen encoding.

Note that this is just an example, and in practice, we would use much larger prime numbers and a larger finite field to ensure the security of the encryption.

10 Conclusion

The recent article is an application of Frobenius rings in the cryptography of health systems. In this article, we have changed the algorithms of RSA, Paillier and Perrin to algorithms with the structures of Frobenius rings, and we have presented some of their applications with concrete examples in the field of health medicine.

References

[1] S. Akhbarifar, H. Haj Seyyed Javadi, A. Rahmani, and M. M. Hosseinzadeh, *A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment*, Person. Ubiquitous Comput. **16** (2020), no. 11, 1–17.

[2] J.L. Alperin, R.B. Bell, J.L. Alperin, and R.B. Bell, *The general linear group*, Groups and Representations, Springer New York, 1995, pp. 39–62.

[3] M. Anzani, H. Haj Seyyed Javadi, and A. Moeni, *A deterministic key predistribution method for wireless sensor networks based on hypercube multivariate scheme*, Iran. J. Sci. Technol. Trans. A: Sci. **42** (2018), 777–786.

[4] P. Asghari, A.M. Rahmani, and H. Haj Seyyed Javadi, *Internet of Things applications: A systematic review*, Comput. Networks **15** (2019), no. 1, 241–261.

[5] J. Berstel, D. Perrin, and C. Reutenauer, *Codes and Automata*, Cambridge University Press, 2010.

[6] P. Charpin, A. Pott, and A. Winterhof, *Finite Fields and Their Applications*, De Gruyter, 2013.

[7] J. Ding, A. Miasnikov, and A. Ushakov, *A linear attack on a key exchange protocol using extensions of matrix semigroups*, preprint. http://eprint.iacr.org/2015/018

[8] E. Di Angelantonio, S.N. Bhupathiraju, D. Wormser, P. Gao, S. Kaptoge, A.B. De Gonzalez, B.J. Cairns, R. Huxley, C.L. Jackson, G. Joshy, and S. Lewington, *Body-mass index and all-cause mortality: individual-participant-data meta-analysis of 239 prospective studies in four continents*, Lancet **388** (2016), 776–786.

[9] Q.F. Hassan, *Internet of Things A to Z: Technologies and Applications*, Wiley-IEEE Press, 2018.

[10] J. Hoffstein, J.H. Silverman, W. Whyte, and Z. Zhang, *A signature scheme from the finite field isomorphism problem*, J. Math. Crypt. **14** (2020), no. 6, 39–54.

[11] B.P.U. Ivy, P. Mandiwa, and M. Kumar, *A modified RSA cryptosystem based on 'n'prime numbers*, Int. J. Engine. Comput. Sci. **1** (2012), no. 2, 63–66.

[12] C. Jost, H. Lam, A. Maximov, and B. Smeets, *Encryption performance improvements of the paillier cryptosystem*, IACR Cryptol. ePrint Arch. **2015** (2015), 864.

[13] J. Kapoor and D. Thakur, *Analysis of symmetric and asymmetric key algorithms*, ICT Analysis and Applications, Springer Singapore, 2022, pp. 133–143.

[14] A.V. Kshirsagar, M. Carpenter, H. Bang, S.B. Wyatt, and R.E. Colindres, *Blood pressure usually considered normal is associated with an elevated risk of cardiovascular disease*, Amer. J. Medic. **119** (2006), no. 2, 133–141.

[15] T.Y. Lam, *Frobenius and quasi-Frobenius rings*, Lectures on Modules and Rings, Graduate Texts in Mathematics, Springer New York, NY, 1999.

[16] I. Mustafa, H. Mustafa, A.T. Azar, S. Aslam, S.M. Mohsin, M.B. Qureshi, and N. Ashraf, *Noise free fully homomorphic encryption scheme over non-associative algebra*, IEEE Access, **8** (2020), 136524–136536.

[17] S. Padmanaban, M. Azimi Nasab, M.E. Shiri, H. Haj Seyyed Javadi, M. Azimi Nasab, M. Zand, and T. Samavat, *The role of Internet of Things in smart homes*, Artific. Intell. Based Smart Power Syst. **25** (2023), no. 1, 259–271.

[18] P. Paillier, *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes*, Berlin, Heidelberg, Springer Berlin Heidelberg, 1999.

[19] L. Qiao and Z. Gao, *Joint active device and data detection for massive MTC relying on spatial modulation*, IEEE Wireless Commun. Network. Conf. Workshops (WCNCW), 2020, pp. 1–6.

[20] J. Rosenthal, *The Hermann-Martin curve*, New Directions and Applications in Control Theory, Lect. Notes Control, vol 321, Springer, Berlin, Heidelberg, 2005, pp. 353–365.

[21] N. Rahman and V. Shpilrain, *A matrix action key exchange*, J. Math. Crypt. **7** (2022), no. 1, 64–72.

[22] V. Rudnytskyi, O. Korchenko, N. Lada, R. Ziubina, L. Wieclaw, and L. Hamera, *Cryptographic encoding in modern symmetric and asymmetric encryption*, Procedia Comput. Sci. **207** (2022), 54–63.

[23] N.H. Shah, D.T. Khan, A.A. Banu, and L.H. Shah, *Symmetric and asymmetric encryption schemes for Internet of Things: A survey*, Int. J. Intell. Syst. Appl. Engin. **11** (2023), no. 1, 254–260.

[24] N. Solari Esfehani and H. Haj Seyyed Javadi, *A survey of key pre-distribution schemes based on combinatorial designs for resource-constrained devices in the IoT network*, Wireless Networks **27** (2021), no. 4, 3025–3052.