Contemporary Mathematics
http://ojs.wiserpub.com/index.php/CM/

UNIVERSAL WISER
PUBLISHER

Research Article

A Secure Key Exchange Protocol and a Public Key Cryptosystem for Healthcare Systems

Yuvasri R, Manimaran A*

Department of Mathematics, School of Advanced Sciences, Vellore Institute of Technology, Vellore, India
E-mail: manimaran.a@vit.ac.in

Received: 16 November 2023; **Revised:** 10 April 2024; **Accepted:** 20 May 2024

Abstract: Diffie-Hellman (DH) is the reason for the existence of a solution to the key distribution problem, where two parties can mutually set up a shared secret key over an insecure channel without any previous communication. In this study, a novel key exchange protocol based on the difficulty of the Discrete Logarithm Problem with Factor Problem ($DLPFP$) utilizing matrices in non-commutative semigroup over semiring is proposed. The security and complexity analyses of the protocol are discussed. Also, an ElGamal cryptosystem based on a group of invertible matrices and $DLPFP$ over a semiring to encrypt the Sensitive Health Information (SHI) in healthcare systems is suggested.

Keywords**:** public key cryptography, key exchange protocol, Diffie-Hellman, ElGamal cryptosystem, semiring

MSC: 11T71, 94A60, 06E20

1. Introduction

Cryptography is the study of private and confidential communication mechanisms that restrict the sender and intended recipient's access to a message's particulars. Recent years have seen the creation of a high volume of data from numerous sources, necessitating secure processing and storage. Personal information about the user and also ubiquitous data collected from many "everyday" gadgets that belong to the cyber world are included in this data. In the healthcare system, due to the ease of combining a variety of health information sources to build a centralized patient record that is quickly accessible, Sensitive Health Information (SHI) has gained popularity among users as a patient-centric model of health information sharing. A patient can create, maintain, and have control over all of her personal health information through a SHI service, which has improved the efficiency of data storage, retrieval, and sharing. The data owner has full control over the SHI. They can also make their health information available to a variety of consumers. A number of privacy and security issues arise during the sharing process, potentially preventing its widespread adoption. The privacy of users is in jeopardy if SHI is kept on a server operated by an unreliable third party. Therefore, encrypting the data is vital. Figure 1 shows the scenario for the healthcare system.

DOI: https://doi.org/10.37256/cm.5220243942

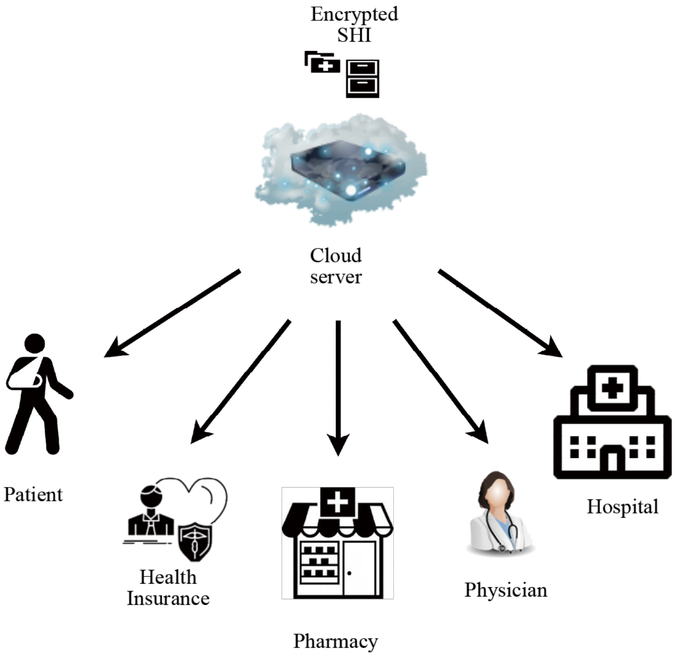

Figure 1. The healthcare system

In the communication between the sender and the receiver, the key exchange algorithm is used to generate the secret key. The safe and secure transfer of the key between the entities is the most difficult task. While exchanging the keys, unauthorized users should not be able to access the information. Whitfield Diffie Hellman and Martin Hellman developed the Diffie-Hellman (*DH*) algorithm in 1976, which facilitated the exchange of private keys between the parties. This algorithm employs the platform group F_p^*, which is the group of integers modulo p under multiplication, where p is prime. It has been proposed that the Discrete Logarithm Problem (*DLP*) and subsequent integer factorization problems are key exchange protocols with essential structures that are quite similar to the *DH* technique previously outlined.

The intractability of problems related to number theory forms the foundation for all of these cryptosystems. Despite their widespread use, these public key techniques suffer from two major flaws. The first is quantum computing's rapid advancement. The creation of a reasonably powerful quantum computer will render certain frequently used public key algorithms, like the Rivest Shamir and Adleman (*RSA*) algorithm, ElGamal, and elliptic curve cryptosystems, no longer secure. The second issue arises from the incompatibility of these number theory-based approaches with small computer hardware, like card readers with low processing speeds.

Despite the fact that quantum computers are still many generations away from being a reality, the cryptography community will soon be on guard against them. As a result, developing faster and more secure non-numerical theory-based cryptographic systems and key exchange methods is critical. In [1], a more effective new type of elliptic curve public key cryptosystem featuring quicker key generation calculations is presented. The Conjugacy Search Problem (*CSP*) [2] over a set of invertible matrices for groups and semigroups is one instance of a challenge that has inspired multiple attempts to build different public key cryptosystems.

In [3], a novel hill cipher is suggested based on vector spaces over non-singular (invertible) matrices. It resolves the known plaintext attack issue. A message exchange protocol based on finite associative-commutative rings with unity characteristics is described in [4]. For the digital signature system described in [5, 6], the general linear group over Z_n and the non-commutative ring are the building blocks. A public key symmetric cipher approach that uses semiring action is proposed in [7]. However, the authors do not explicitly state the security of this scheme. Stickel's key exchange protocol in tropical algebra was updated by the authors [8] utilizing commuting matrices, and they also proposed additional protocols.

The basis for our study is a non-commutative group of invertible matrices over semirings. As a result of including all the highlights, our suggested scheme's security has improved.

Based on the premise of a strong computational DH without sacrificing security, [9] offers a tight security key exchange technique. A new modified and enhanced DH non-commutative key exchange mechanism is proposed in [10]. It protects against linear algebra attacks as well as both linear and non-linear decomposition attacks. For increased data privacy and integrity, a revised encryption technique built on the DH approach is suggested in [11]. It protects against man-in-the-middle attacks and discrete logarithm attacks. Only a few known attacks explain the security of these schemes, as they fail to overcome many others.

In [12, 13], a modified algorithm based on the ElGamal and Cramer-Shoups cryptosystems is presented. In [14], a simple, lightweight, and efficient encryption scheme is given. An updatable ElGamal encryption scheme that achieves forward and backward security for cloud storage is proposed in [15]. In [16–18], an ElGamal scheme and key exchange protocols for the Internet of Things environment are designed. In [19, 20], cryptosystems using blockchain are proposed. Some encryption schemes for enhancing the security of healthcare systems are given in [21–24].

Our protocol is based on a set of invertible matrices over a finite field. A non-invertible key exchange protocol over a ring is suggested by the author in [25] and affirms that it takes less time than DH, ElGamal, and RSA. In the view of [2, 26], the DLP on $GL_n(F_r)$ is converted into a basic factoring issue or a DLP over finite fields [26] due to attacks like determinant attack, eigenvalue attack, and the Cayley-Hamilton attack. A platform is suggested to get around this conversion problem. It is made up of the semigroup of matrices over group ring $M_{n \times n}(F_r[S_r])$ under normal matrix multiplication [27] and the group of invertible matrices over group ring $GL_n(F_r[S_r])$ [28]. [29] claims that the "semi-simple algebra" structure of group rings can decipher the key exchange protocols based on DLP. [30] suggests a Factorization Discrete Logarithm Problem ($FDLP$)-based key exchange protocol and analyses the security and complexity. Also, an ElGamal cryptosystem is proposed. In [31], this protocol's security is examined thoroughly. A modified RSA algorithm to encrypt the SHI is proposed in [32]. Our approach is based on a group of invertible matrices over semiring, which is a more feasible generalization of the group ring. Our approach fixes the flaws in the previously discussed systems.

Recently, several attempts were made to secure the SHI by using cryptographic protocols. However, to our best knowledge, a few of them have provided these protocols based on ElGamal cryptosystems and mathematical hard problems. In [30], a protocol based on the group of invertible matrices over group rings is presented. Semiring is a generalized concept of group rings. This motivates us to design a new problem, Discrete Logarithm Problem with Factor Problem ($DLPFP$), upon which we construct a key exchange protocol and an ElGamal cryptosystem using matrices in the non-commutative semigroup over semiring to secure the SHI. The proposed protocol is more secure but has the same time complexity. Also, we have enhanced our scheme by concealing the subsemigroup.

In this study, we attach a hidden parameter to the ideas of the DLP and Factor problem (FP) over a non-commutative semigroup $M_{n \times n}(R_s)$, which becomes the $DLPFP$ problem. Using the above-given attacks does not reveal the secret key, making the suggested protocol more efficient than previously published protocols. Then, a key exchange protocol is proposed based on this $DLPFP$. We have presented the protocol's complexity and security measures. Also, based on $DLPFP$ over a group of invertible matrices, an ElGamal cryptosystem for encrypting the data in the healthcare system is proposed.

The order of the paper's sections is as follows: The terms DLP, FP, $DLPFP$, centralizer, and semiring are defined, and the model, structure, flow, and security goals of the system and the list of notations used are given in Section 2. In Section 3, a key exchange protocol based on $DLPFP$ is proposed along with a theorem. In Section 4, the proposed protocol's security and complexity are evaluated. Using the group of invertible matrices over a semiring, an ElGamal cryptosystem for SHI is proposed, with an example in Section 5. Lastly, in Section 6, the paper is concluded.

2. Preliminaries

In this section, DLP, FP, $DLPFP$, Centralizer, and Semiring are defined [30, 33, 34], and the model, structure, flow, and security goals of the system are given.

2.1 *Basic definitions*

Definition 1 (*DLP* [30]) Let p be a prime and given an element $\beta \in F_p^*$ where F_p^* is a cyclic group of order $p-1$ generated by α, find an integer e, $0 \leq e \leq p-1$ such that $\alpha^e \equiv \beta \bmod p$.

Definition 2 (*FP* [30]) Given an element g from non-abelian semigroup G and two subsemigroup of G namely H_1, and H_2, find two elements $h_1 \in H_1$ and $h_2 \in H_2$ such that $g = h_1.h_2$.

Definition 3 (*DLPFP*) Given an element g from non-commutative semigroup G and two subsemigroup of G namely H_1, and H_2, find three elements $h_2 \in H_2$ and t, $s \in Z_r^*$ where r is an integer such that $g = h_1^t.h_2^s$.

Example Let $GL_3(Z)$ be a non-abelian semigroup and the subsemigroup of $GL_3(Z)$ be the set of all 3×3 diagonal matrices. Also, let Z_r^* be Z_{11}^*. Consider the equation $g = h_1^t.h_2^s$ where the given values are $t = 2,\ s = 3$,

$$g = \begin{bmatrix} 733 & 1,253 & 1,238 \\ 420 & 700 & 704 \\ 207 & 355 & 350 \end{bmatrix} \in GL_3(Z),$$

$$h_1 = \begin{bmatrix} 3 & 4 & 1 \\ 1 & 4 & 0 \\ 1 & 1 & 0 \end{bmatrix} \in GL_3(Z),$$

$$h_2 = \begin{bmatrix} 2 & 5 & 3 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \in GL_3(Z).$$

Now, the problem is to find the values of h_2, t, and s from the above equation.

Definition 4 [33] For an element $g \in G$, let $C(g)$ be the set of elements that commute with g, i.e., $C(g) = \{a \in G : ga = ag\}$. $C(g)$ is called the centralizer of g in G.

Definition 5 [34] A non-empty set R_s is called a semiring if the operations of addition and multiplication are defined in the following ways:

(i) $(R_s, +)$ is a semigroup;

(ii) $(R_s, \bullet)$ is a semigroup;

(iii) $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$ for every a, b, $c \in R_s$.

2.2 *System model*

The proposed system model consists of the data owner, i.e., the Patient (P_a), Personal Domain (P_eD), Public Domain (P_uD), Administrator (A_d), and Big Data Server (S). The categorizations of the model are given in Figure 2 and are described as follows:

P_a: The details of P_a like name, date of birth, gender, address, contact number, disease, etc., are registered in the system and are stored in S.

P_eD: The domain includes family members and friends who are very close to P_a. They are granted access rights by P_a in accordance with the required conditions.

P_uD: The domain includes parties like insurance providers, additional hospitals, etc. The parties cannot access the SHI until P_a gives permission.

A_d: First, when P_a enters the hospital for treatment or consultation, he or she is asked to provide the details for their profile and also register. The registration ID and private key (updated each time) are provided to P_a by A_d.

S: The SHI of P_a is stored here. S makes storing, processing, and analyzing enormous amounts of data simple. In this paper, the server is considered semi-honest.

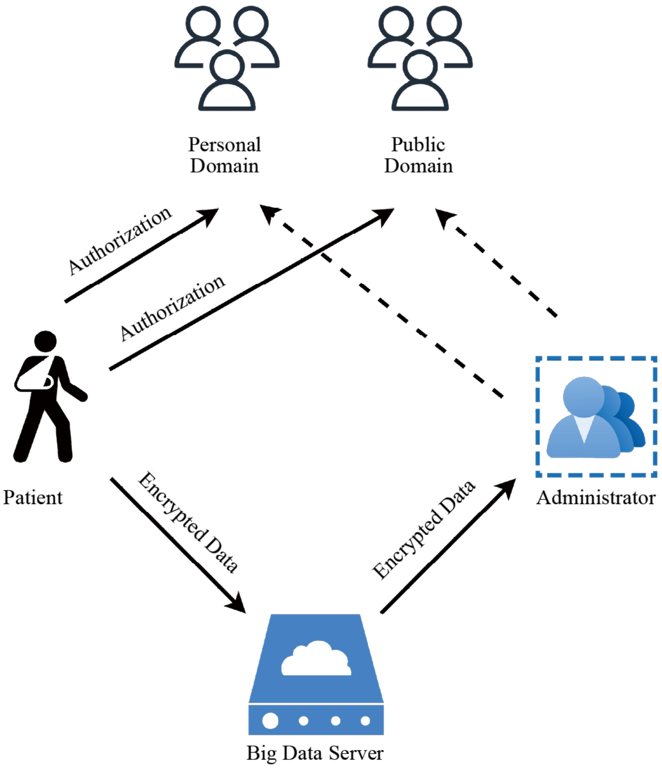

Figure 2. The system model

2.3 *Structure and flow of the proposed protocol*

Three roles are specified for handling P_a health data: a doctor, a nurse, and a staff member. A doctor has the ability to add, edit, or remove the treatment records of P_a. He or she is granted access to the entire medical records (SHI) of the P_as that are allocated to them. A nurse also has access to and control over SHI, but with fewer privileges this time. In particular, a nurse is able to add information to the SHI. However, their access to the visit histories of P_a is limited, preventing them from viewing specific medical records of doctors assigned to them. The third role owner, i.e., the staff member, can view the basic information, including his identity, visit date, time, and cost. The staff allocates the P_a to a suitable and accessible healthcare professional and keeps track of how long they wait. The A_d is in charge of creating roles, assigning users to these jobs, and handling role granting and revocation, for example, by recruiting or firing doctors, nurses, and other staff members. The workflow of the proposed protocol is described as follows:

During the first visit, P_a provides A_d with profile details. A_d uploads it in S. When registering, P_a specifies the members of P_eD. The access privileges of P_eD members are specified by P_a. P_a also clearly knows about the individuals who have access to P_uD. If someone wants to access SHI, then a secret key request is sent to P_a, and he or she approves or declines the request. The SHI is encrypted under a domain-based access policy and stored in S. It is decrypted by P_a, or the authorized user with the private key. The users are those who are specified in the public or private domain with access rights. The individuals from P_eD are close friends and family members. Therefore, P_a allows them to access the data with respect to their relationship.

2.4 *Security goals*

The main aim of the patient-centered scheme is that the P_a should have control over his or her SHI. In order to achieve this, the system needs to maintain data confidentiality, integrity, adaptability, scalability, and efficiency. They are described as follows:

1. Confidentiality: The decryption of the SHI file is done only by authorized individuals, as mentioned by P_a. Unauthorized individuals lacking the necessary access privileges cannot decrypt the SHI.

2. Integrity: Preventing unauthorized individuals from gaining access to modify the data.

3. Adaptability: It is necessary for the access policy to be flexible when it is characterized by constant change.

4. Scalability: The system must encourage the P_eD and P_uD users. Even if the size of the P_uD increases, the system must support it. Also, high adaptability and applicability are required.

5. Efficiency: It is necessary to minimize the effort required to handle the clients and keys.

3. A key exchange protocol based on *DLPFP*

In this section, a *DLPFP*-based key exchange protocol that employs matrices over semiring is proposed, and a theorem is established.

The Protocol: Assume that under multiplication, $A = M_{n\times n}(R_s)$ is a finite non-commutative semigroup. Let B be a commutative subsemigroup of A, and $F_r^* = \{1,\ 2,\ 3,\ \ldots,\ r-1\}$, where r is a big positive integer. Suppose $a \in A$ and $C_A(a)$ is the centralizer of a in A. The public parameters are A, a, and r. Let the parties involved in the key exchange protocol be Alice and Bob, who know the public information. The following is the proposed protocol:

(1) Alice computes $C_1 = a^i y^j$, where the secret parameters i, j, and y are chosen from F_r^* and $B\setminus C_A(a)$, respectively. $B\setminus C_A(a)$ contains all the elements in B except the ones that commute with a. Alice sends C_1 to Bob.

(2) Bob computes $C_2 = a^k z^l$ where the secret parameters k, l and z are chosen from F_r^* and $B\setminus C_A(a)$, respectively. Bob sends C_2 to Alice.

(3) Alice calculates $K_1 = a^i C_2 y^j$.

(4) Bob calculates $K_2 = a^k C_1 z^l$.

The exchanged secret key (K) is $K_1 = a^i C_2 y^j = a^{i+k} z^l y^j = a^{k+i} y^j z^l = a^k C_1 z^l = K_2 = K$ because of the commutative property of y and z, that is, $yz = zy$ in B.

In the healthcare system scenario, the key exchange takes place between the P_a or the users from P_uD or P_eD (whoever requests the SHI of P_a) and the A_d. The P_a or the users from P_uD/P_eD perform Alice's part during the key exchange. Bob's part is done by the A_d. In order to create a different key each time, the matrix y is calculated as follows: The alphabets in the P_a and the consulting doctor's password are converted into numerical values, and the corresponding binary value is calculated. Now, the first binary value of P_a's password and the doctor's password are added using the logical operator $\oplus$. Then, the resulting binary value is again converted into a numerical value, which is the first entry of the matrix y. The same method is followed to calculate each value. According to the size of the matrix (y), entries are added or deleted randomly.

Remark The constraint that y and z do not commute with a cannot be modified since if $ay = ya$ or $az = za$, then the secret key is easily found by the adversary because

$$K_1 = a^i C_2 y^j = a^i a^k z^l y^j = a^i y^j a^k z^l = C_1 C_2$$

or the other way, that is,

$$K_2 = a^k C_1 z^l = a^k a^i y^j z^l = a^k z^l a^i y^j = C_2 C_1.$$

This is because the values of C_1 and C_2 are sent through an insecure channel.

Remark Let us assume that $za = az$ and $y,\ z \in B \setminus C_A(a)$. $C_A(a)$ is the centralizer of a in A, and it contains all the elements in A that commute with a. Here, $B \setminus C_A(a)$ contains all the elements in B except the ones that commute with a. This contradicts our assumption. Therefore, $za \neq az$. Also, y and z belong to $B \setminus C_A(a)$, where B is a commutative subsemigroup. Therefore, $yz = zy$.

Remark In the above protocol, another way of choosing y is from $A \setminus C_A(a)$ and proceeding with another modification, i.e., by selecting the secret polynomials $F_q[x]$ such that $f(x)$ and $g(x)$ commute with each other and the key is also calculated in the same way, that is

$$C_1 = a^i f(y)^j \text{ and } C_2 = a^k g(y)^l.$$

Theorem 1 Let $A = M_{n\,\times\,n}(R_s)$ be a finite non-commutative semigroup under multiplication over semiring R_s and let $F_r^* = \{1,\ 2,\ 3,\ \cdots,\ r-1\}$, where r is a big positive integer. If the key exchange protocol is based on $DLPFP$, then the keys are exchanged securely through the protocol when B is a commutative subsemigroup of A.

Proof. Given that $A = M_{n\,\times\,n}(R_s)$ is a finite non-commutative semigroup over semiring, under usual matrix multiplication, and B is a subsemigroup of A, where $B = \{N_{n\,\times\,n}(R_s)\}$. $F_r^* = \{1,\ 2,\ 3,\ \ldots,\ r-1\}$ where r is a big positive integer and $a \in A$, and $y,\ z \in B \setminus C_A(a)$.

To prove: The key exchange is securely done based on $DLPFP$ when B is chosen as a commutative subsemigroup of A and $a \in A$, and $y,\ z \in B \setminus C_A(a)$.

According to the key exchange protocol, let $a \in A$ and $C_A(a)$ be the centralizer of a in A. Now, the parameters in the public domain are A, a, and r. Assume that the people transferring keys are Alice and Bob.

The key exchange is as given in the above Key Exchange Protocol based on $DLPFP$. The exchanged secret key K is $K_1 = a^i C_2 y^j = a^{i+k} z^l y^j$, and $K_2 = a^k C_1 z^l = a^{k+i} y^j z^l$. Therefore, $K_1 = K_2 = K$ (since B is commutative). The key exchange is successful.

Let us assume that the key exchange is insecure, i.e., with knowledge of the exchanged values (C_1, C_2) and the public parameters (A, a, and r), the adversary can deduce the secret keys. To compute the secret key $K_1 = a^i a^k y^k z^l$ with the known values, the adversary calculates $C_1 C_2 = a^i y^k a^k z^l$. To equate the values of $C_1 C_2$ and K_1, y must commute with a. This, however, contradicts our assumption that $ya \neq ay$. So even if the adversary intercepts the exchanged values and knows the public parameters, deducing the secret keys remains infeasible due to the non-commutative property of the elements involved. Therefore, the key exchange is secure. □

4. The security analysis and complexity analysis

In this section, the security analysis of the $DLPFP$-based key exchange protocol is examined, and the number of operations required to run this protocol is analyzed along with the time complexity graph.

4.1 *The security analysis*

The security and time complexity of the suggested $DLPFP$ key exchange protocols are examined in this section.

Assuming that the above problem is computationally difficult, our Section 3 protocol is secure: It is difficult to calculate the shared key K given the public data a, C_1, and C_2. This is the protocol's computational assumption. The tougher decisional version of this condition is: It is challenging to tell the shared key K from an arbitrary element of the type $a^k m$ given a, C_1, and C_2. The security evaluation of our protocol against many forms of attacks, some of which are published in [2, 26, 29, 35], is provided below:

(i) Attacks by using matrices' characteristics: FDLP is resistant to the Cayley-Hamilton attack [26], the determinant attack [2], and the eigenvalue attack. The eigenvalue attack is irrelevant since a's eigenvalues are identified but not those of a^i. The non-commutative determinant prevents the determinant attack from working [2]. In contrast to situations where *DLP* is the root cause of the issue, det(a^iy^j) and det(a) are known, but currently, there are three unknown variables (i, j, and y). Since y is unknown, this approach is not suitable to determine i or j. To use the Cayley-Hamilton attack, you must know $a, y \in M_{n \times n}(R_s)$ such that $a^iy^j = g(a)h(y)$, such that $g(x),\ h(x) \in R_s$ and

$$g(x) = \sum_{i=0}^{r-1} b_i a^i,\ \ h(y) = \sum_{i=0}^{r-1} c_i y^i.$$

Since y and j are not known, it is unattainable to detect $h(y)$. Therefore, the Cayley-Hamilton attack cannot solve this.

(ii) Attacks over *DLP*: To solve the *DLP*, numerous algorithms were introduced. Our underlying problem is *DLP*, and the algorithms cannot be used in our protocol since in *DLP*, a is known and a^i is unknown, so it was broken through the algorithms. But, here, "i" is hidden using two parameters, y and j, which are confidential such that $C_1 = a^iy^j$ and the subsemigroup B is hidden as given in [33], which makes it more difficult for the adversary to attack.

(iii) Brute force attack: For given a_1, a_2, and $a_3 \in A$ and $t,\ s \in F_r^*$, $a_1 = a_2^t\ a_3^s$ and in F_r^*, r is a big positive integer, where $A = \{d_1,\ d_2,\ \ldots,\ d_\alpha\}$ is a non-commutative semigroup of α elements. The elements of A are expressed as $a_1 = d_{i_1}$, $a_2 = d_{i_2}$, and $a_3 = d_{i_3}$ for some $i_1, i_2, i_3 \in \{1,\ 2,\ \ldots,\ \alpha\}$. α is the number of options for a_3, and r is the number of options for a_1 and a_2. By brute force attack, to solve the *DLPFP*, the steps involved are $O(\alpha r) = \alpha r$ bits, which is exponential. $\alpha r = e^{log_e \alpha r} = e^{log_e 2.log_2 \alpha r} = e^{f.size(\alpha r)}$ and $f = log_e 2$. This grows reasonably fast as the values of α and r increase. Therefore, brute force attack is not possible.

```
Algorithm 1 Exhaustive search algorithm
Input: Let $a \in A$ such that $C_1 = a^iy^j$, and $C_2 = a^kz^l$
Output: Secret parameters: $B \subset A$, $y, z \in B \setminus c_A(a)$, $i, j, k, l \in F_r^*$, $K_1$, and $K_2$
  for $i \leftarrow 1$ to $r-1$ do
    for $j \leftarrow 1$ to $r-1$ do
      $K_1 \leftarrow a^iy^j$;
      for $k \leftarrow 1$ to $r-1$ do
        for $l \leftarrow 1$ to $r-1$ do
          $K_2 \leftarrow a^kz^l$;
          compare $K_1 = K_2$;
          if $K_1 = K_2$; then
            return $K_1 = K_2$ & exit;
          else
            go to next step;
          end if
        end for $i \leftarrow i+1$
      end for $j \leftarrow j+1$
    end for $k \leftarrow k+1$
  end for $l \leftarrow l+1$
```

For the key exchange protocol based on *DLPFP*, an exhaustive search method is provided in Algorithm 1.

(iv) Linear algebra attack: Only in the following way, our strategy is compatible with the linear algebra attack described in [36]:

1. Find a matrix u with the property $ua = au$.

2. Find a matrix v with the condition $vz = zv$. Because it is abelian, such a matrix v is chosen from the hidden subsemigroup B.

3. C_1, u, and v should satisfy the equation $C_1 = uv$.

Then, the secret key can be evaluated as:

$$uC_2v = ua^k z^l v = a^k uvz^l = a^k C_1 z^l.$$

This value matches the secret key. At least one solution exists for this method, i.e., $u = a^i,\ v = y^j$. The solution for the group of matrices over semirings is given below.

(1) To find u such that $ua = au$: Let us consider the set of all 2×2 matrices. Suppose the adversary knows the matrix $a = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$ and has to find the unknown matrix $u = \begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix}$ so that it satisfies $ua = au$. Now, we have four equations while solving $ua = au$, i.e., $a_1u_1 + a_2u_3 = u_1a_1 + u_2a_3$, $a_1u_2 + a_2u_4 = u_1a_2 + u_2a_4$, $a_3u_1 + a_4u_3 = u_3a_1 + u_4a_3$, and $a_3u_2 + a_4u_4 = u_3a_2 + u_4a_2$. If the elements are taken from a commutative group, they are linear equations with variables that are unknown, i.e., $a_2u_3 - u_2a_3 = 0$, $a_1u_2 + (u_4 - u_1)a_2 - u_2a_4 = 0$, $a_3u_1 + (a_4 - a_1)u_3 - u_4a_3 = 0$, and $a_3u_2 - u_3a_2 = 0$. This reduces to $qt = 0$ for some matrix q and $t = [u_1u_2 \ldots u_n]^i$ where $u_1,\ u_2,\ \ldots,\ u_n \in u$. If the elements are taken from a non-commutative group, then it is not possible for the equations to be linear since $ua \neq au$. As given in (iii) above, a brute force attack is not applicable here, even if the equations are written in linear form, because by brute force attack, the number of steps required is $O(\alpha r)$ bits (exponential), and it grows reasonably fast as the size of the platform increases. Also, invertibility is not mandatory for the matrix q. The restrictions we have made disable the attacks on finding u. Also, the basic platform where y, z is taken from B and is hidden. Therefore, the adversary remains unaware of the origin of these matrices.

(2) To find v such that $vz = zv$: To find v from the hidden subsemigroup B is not possible as discussed in [30] and (1) above. It will also not work out, as in the case of Remark 2, since the commutative subsemigroup B is hidden.

(3) Solving the equation $C_1 = uv$: The known matrix is C_1. The matrices u and v are unknown, where $u = a^i$ and $v = y^j$ (since $C_1 = x^i y^j$). The secret parameters are y, i, and j. It is considered a hard problem.

A system of quadratic equations is produced by solving the matrices, as shown in [30]. The only way to find the resolution is by using a brute force attack. However, convincing evidence has demonstrated that the time complexity of solving quadratic equations remains safe from this attack.

(v) Ciphertext only attack: The value of $C_2 = a^k z^l$ is used as the ciphertext C_2 in the ElGamal Public Key Cryptosystem 5. Therefore, the ciphertext only attack can be used on C_2 here. In the ciphertext only attack, the adversary only knows C_1 or C_2. An adversary knows only the matrices C_1, C_2, and a, which are public parameters. To find the plaintext o, he must first find the unknown matrices y, z, K_1, and K_2. He assumes random matrices $y = y_1$ and $z = z_1$. Therefore, $C_1 = a^i y_1^j$. In the same way, $C_2 = a^k z_1^l$. Here, he has a large system of nonlinear equations for the ciphertext corresponding to each plaintext. He finds the corresponding solution, $o = o'$. Thus, for each fixed $y = y_1$, the adversary gets a number of $(C_1',\ C_2',\ z_1,\ o')$. This process generates a large system of equations with a large number of unknowns. No matter how an adversary rearranges these equations, the problem of having a product of two unknown matrices persists. This solution becomes infeasible.

(vi) Known plaintext attack: Here, the adversary knows the ciphertext $C = (C_1,\ C_2)$ corresponding to the plaintext o_i for $(i = 2,\ 3,\ 4,\ \ldots,\ j)$. Let the plaintext-ciphertext pair be $(o,\ C)$. He wants to find the next plaintext, $o_{j\,+\,1}$, that corresponds to the ciphertext, $C_{j\,+\,1}$, from this plaintext-ciphertext pair. In the proposed public key cryptosystem, these types of attacks are impossible because different keys are used to encrypt every new plaintext. Hence, it does not provide any information about the next unknown plaintext-ciphertext pair. As a result, we have demonstrated that our proposed cryptosystem is secure against known plaintext attack. As discussed earlier, brute force attack is also impossible.

(vii) Man in the middle attack: In [33], the man in the middle attack is beaten by two enrichments. We conceal the subsemigroup B and discreetly select the matrix y from B and the matrix z from B, respectively, to enhance the security of our proposed system. The location where y and z are selected from is not reflected here, making it challenging for the foe to locate B. So, as previously described, it is a secure protocol.

4.2 *The complexity analysis*

The time taken to perform the $DLPFP$ algorithm is evaluated in this subsection. The computational time to calculate the shared key, i.e., the number of operations essential in bits, is determined as follows:

1. To multiply two matrices of rank n, $O(n^3)$ bit operations are required.
2. To calculate the matrix a raised to the power of i, it takes $n^3 logr$ number of bit operations.
3. In order to determine $C_1 = a^i y^j$, it is necessary to do $n^3 logr + n^3 logr + n^3 = 2n^3 logr + n^3$ bit operations.
4. To evaluate $a^k C_1 z^l$, the number of bit operations needed is $n^3 logr + 2n^3 logr + n^3 + n^3 logr + 2n^3 = 4n^3 logr + 3n^3$.
5. To calculate the secret key, the total number of bit operations required is $2n^3 logr + n^3 + 4n^3 logr + 2n^3 = 6n^3 logr + 3n^3$. $6n^3 logr + 3n^3$ is proportionally equal to $O(n^3 logr)$.

The time complexity to calculate the key K in the DH process requires $O((log_2 r)^3)$ bit operations where the elements are taken from the commutative group F_r^*. Here, the time complexity is $O(n^3 logr)$ because the entries of the key are taken from the semiring, and to evaluate the shared key, four matrices are to be multiplied. The semigroup $M_{n\,\times\,n}(R_s)$ has η elements, and the matrices are simply raised to the powers of the F_r elements. So, the time complexity for an exhaustive search is $O(\eta r)$. The protocol is strong enough to withstand attacks using eigenvalues and determinants [2] because it employs the semigroup $M_{n\,\times\,n}(R_s)$.

The time complexity of the key exchange protocol based on $DLPFP$ and $FDLP$ [30] is compared in Figure 3. The x-axis represents the order of the matrix (n). The y-axis represents the order of time complexity of the key exchange protocol based on $DLPFP$ ($O(6n^3 logr + 3n^3)$) and $FDLP$ ($O(2n^3 logr + 3n^3)$). Here, r = 13. The red and blue curves represent the time complexity of the key exchange protocol based on $DLPFP$ and $FDLP$, respectively. As the order of the matrix increases, the time complexity also increases. There is a minuscule difference in the slope of the curves, and it is because of the coefficient present in the time complexity of both protocols. But the time complexity of both protocols is proportional to $O(n^3 logr)$.

The advantage of the proposed protocol is that the total operations needed to run the proposed program is the same as the $FDLP$, and the security of the proposed key exchange protocol is more promising because of the inclusion of the secret parameters i, j, y, z and the hidden commutative subsemigroup. Additionally, our protocol overcomes some attacks, which makes it impossible to attack using the known methods.

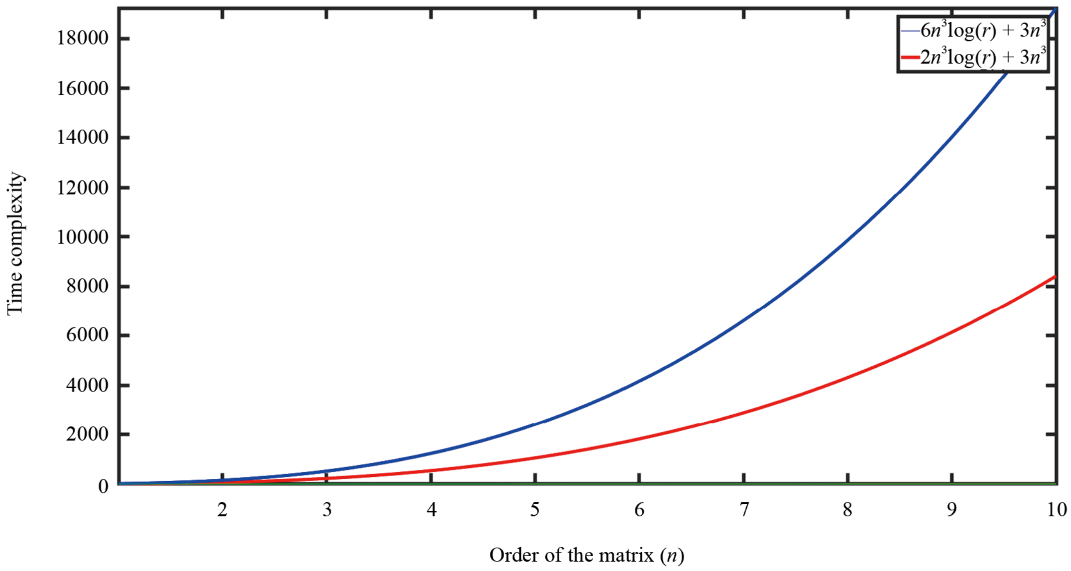

Figure 3. Comparison between the time complexity of the Key exchange protocols based on $DLPFP$ and $FDLP$

5. ElGamal public key cryptosystem

This section introduces an ElGamal public key cryptosystem that is based on the suggested key exchange mechanism. Also, a theorem is given stating that solving the *DLP* and this ElGamal cryptosystem are the same.

Let $A = M_{n \times n}(R_s)$ be a finite non-commutative semigroup under multiplication. Let B be a commutative subsemigroup of A and $F_r^* = \{1, 2, 3, \ldots, r-1\}$, where r is a big positive integer. To encrypt and decrypt, the following ElGamal cryptosystem is used. A flowchart for the proposed cryptosystem is given in Figure 4.

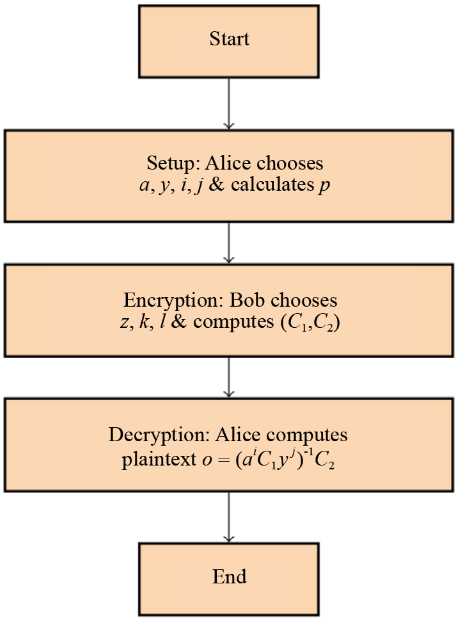
Start
Setup: Alice chooses a, y, i, j & calculates p
Encryption: Bob chooses z, k, l & computes (C_1, C_2)
Decryption: Alice computes plaintext $o = (a^i C_1 y^j)^{-1} C_2$
End

Figure 4. Flowchart for the proposed ElGamal cryptosystem

Setup Alice and Bob are the two classical entities taking part in the communication, and suppose a message is being sent by Bob to Alice. First, Alice does the following to compute her public key: Alice chooses $a \in A$, such that $a^q = I$, where q is the order of a, and selects $y \in B \setminus C_A(a)$ and $i, j \in F_r^*$ and calculates $p = a^i y^j$. Alice's secret key is $S_k = (i, j, y)$, and her public key is $P_k = (p, a)$.

Encryption Bob performs the following computations to encrypt the plaintext:

1. Bob chooses $z \in B \setminus C_A(a)$ and $k, l \in F_r^*$ and keeps it secret. He computes $C_1 = a^k z^l$.
2. The original plaintext is given in the form of a matrix $o \in M_{n \times n}(R_s)$.
3. $C_2 = a^k p z^l o$ is calculated by Bob, and the ciphertexts (C_1, C_2) are sent to Alice.

Note that the matrix o is chosen in such a way that C_2 is non-zero.

Decryption Alice decrypts the original plaintext message o by calculating

$$o = (a^i C_1 y^j)^{-1} C_2$$

since

$$
\begin{aligned}
(a^iC_1y^j)^{-1}C_2 &= (a^ia^kz^ly^j)^{-1}a^kpz^lo \\
&= (a^{i+k}z^ly^j)^{-1}a^kpz^lo \\
&= (a^kpz^l)^{-1}a^kpz^lo \\
&= o.
\end{aligned}
$$

The matrices a, y, and z are chosen in such a way that they are invertible. Therefore, C_1 and $a^iC_1y^j$ are also invertible. Hence, the original plaintext can be decrypted by using these invertible matrices.

Remark Clearly, to encrypt and decrypt, the matrix o need not be invertible.

In the case of healthcare systems, the encryption and decryption of SHI are as follows: The P_a gives the details, and his or her profile is encrypted and uploaded in S by A_d. When the P_a gives the details, he/she also does the part of Alice as given in Section 5. If the authorized users of P_eD or the users of P_uD request P_a's SHI data, then they will do the part of Alice. That is, the authorized users who want to decrypt the data do the work of Alice in Section 5, and A_d does the work of Bob. Then, the P_a, or the authorized users, get to decrypt the SHI file.

Theorem 2 The Diffie-Hellman Problem (*DHP*) can be broken if the above mentioned ElGamal public key cryptosystem can be cracked.

proof. We have to prove

(i) Solving the *DHP* is all that is required to crack the ElGamal public key cryptosystem.

(ii) To crack the *DHP*, it is enough to solve the ElGamal public key cryptosystem.

(i) Suppose, Eve is the attacker who can approach the *DHP* oracle, represented as DHP_o.

Here, the values of $p = a^iy^j$ and $C_1 = a^kz^l$ are appealed to the DHP_o by Eve. The oracle replies back with the value $K = a^{i+k}z^ly^J$, that is,

$$
DHP_o(a^iy^j,\ a^kz^l) = a^{i+k}z^ly^J.
$$

Eve can decrypt and find the original plaintext message (o). The ElGamal cryptosystem can be broken, as the attacker can calculate $o = K^{-1}C_2$ by computing K^{-1}.

Therefore, it is sufficient to crack the *DHP* in order to crack the ElGamal cryptosystem.

(ii) In order to prove (ii), we assume that an attacker, Eve, who can access an ElGamal oracle exists. The oracle reveals the value of o by taking the values of p, C_1, and C_2, where $p = a^iy^j$, $C_1 = a^kz^l$, and $C_2 = a^kpz^lo$. Since

$$
C_2 = pC_1o,
$$

$$
o = C_2(pM_1)^{-1}.
$$

As, $K = a^{i+k}z^ly^J = M_2o^{-1}$.

The attacker computes K, as o is known [37].

Therefore, solving the *DHP* just requires breaking the ElGamal cryptosystem. □

5.1 *A toy example*

A toy example to illustrate our proposed public key cryptosystem is given in this subsection.

Let the semiring $R_s = Z$,

$$A = M_{4\times 4}(Z) = \left\{ \begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix} : a,\ b,\ c,\ d,\ e,\ f,\ g,\ h,\ i,\ j,\ k,\ l,\ m,\ n,\ o,\ p \in Z \right\},$$

$$B = \left\{ \begin{bmatrix} q & 0 & 0 & 0 \\ 0 & r & 0 & 0 \\ 0 & 0 & s & 0 \\ 0 & 0 & 0 & t \end{bmatrix} : q,\ r,\ s,\ t \in Z \right\} \text{ and } F_{59}^{*} = \{1,\ 2,\ \ldots,\ 58\}.$$

Setup

1. Alice chooses

$$a = \begin{bmatrix} 5 & 7 & 2 & 4 \\ 3 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 4 \end{bmatrix} \in A,\ y = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \in B \setminus C_A(a),$$

and $i = 5$, and $j = 4 \in F_{59}^{*}$.

2. Alice calculates

$$p = a^i y^j = \begin{bmatrix} 701,360 & 45,643 & 1,665,279 & 43,184 \\ 290,208 & 18,833 & 688,095 & 17,812 \\ 173,648 & 11,306 & 412,290 & 10,691 \\ 208,000 & 13,533 & 498,474 & 13,073 \end{bmatrix}.$$

Encryption

1. Bob chooses

$$z = \begin{bmatrix} 5 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \in B \setminus C_A(a),\ k = 2,$$

and $l = 3 \in F_{59}^{*}$.

2. Bob calculates

$$C_1 = a^k z^l = \begin{bmatrix} 6{,}500 & 50 & 621 & 45 \\ 2{,}500 & 25 & 243 & 18 \\ 1{,}625 & 12 & 162 & 11 \\ 1{,}625 & 14 & 216 & 22 \end{bmatrix}.$$

3. Suppose, Bob wants to send the message “BANK DETAILS OF A”, he converts it into the matrix

$$o = \begin{bmatrix} 1 & 0 & 13 & 10 \\ 3 & 4 & 19 & 0 \\ 8 & 11 & 18 & 14 \\ 5 & 0 & 0 & 0 \end{bmatrix} \in A$$

by assigning the values 0 to 25 to the alphabets A to Z.

4. Bob calculates $C_2 = a^k p z^l o$.

$$C_2 = \begin{bmatrix} 41{,}103{,}545{,}785 & 45{,}431{,}974{,}062 & 178{,}939{,}755{,}459 & 138{,}219{,}991{,}524 \\ 16{,}986{,}320{,}616 & 18{,}774{,}671{,}941 & 73{,}951{,}226{,}769 & 57{,}122{,}774{,}666 \\ 10{,}177{,}629{,}323 & 11{,}249{,}372{,}353 & 44{,}307{,}321{,}432 & 34{,}224{,}688{,}538 \\ 12{,}240{,}965{,}335 & 13{,}532{,}352{,}165 & 53{,}271{,}243{,}335 & 4{,}114{,}887{,}449 \end{bmatrix}.$$

5. Bob sends the ciphertext (C_1, C_2) to Alice.

Decryption

1. Alice retains the original message matrix o by calculating $o = (a^i C_1 y^j)^{-1} C_2$.

$$o = \begin{bmatrix} 8{,}041{,}878{,}000 & 4{,}184{,}109 & 4{,}128{,}657{,}966 & 3{,}970{,}346 \\ 3{,}323{,}654{,}000 & 1{,}729{,}033 & 1{,}706{,}159{,}619 & 1{,}640{,}513 \\ 1{,}991{,}258{,}000 & 1{,}036{,}054 & 1{,}022{,}293{,}467 & 983{,}085 \\ 2{,}393{,}222{,}000 & 1{,}245{,}195 & 1{,}229{,}761{,}035 & 1{,}183{,}894 \end{bmatrix}^{-1} \times C_2$$

$$o = \begin{bmatrix} 1 & 0 & 13 & 10 \\ 3 & 4 & 19 & 0 \\ 8 & 11 & 18 & 14 \\ 5 & 0 & 0 & 0 \end{bmatrix}.$$

2. Alice converts the matrix o into the message.

If $B \setminus C_A(a)$ were empty, it would mean every element in B commutes with a (i.e., $B \subseteq C_A(a)$). If all elements in B commute with a, then the chosen secret elements (y and z) also commute with a. This compromises the security of the protocol. The adversary could potentially calculate the secret key (K) from the intercepted messages (C_1 and C_2) by exploiting commutativity.

Consider B as the set of all diagonal matrices. Due to matrix multiplication principles, the elements of B do not commute with matrices in A that contain non-zero off-diagonal elements. Therefore, $B \setminus C_A(a)$ is nonempty.

Let

$$A = M_{4\times 4}(Z) = \left\{ \begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix} : a,\, b,\, c,\, d,\, e,\, f,\, g,\, h,\, i,\, j,\, k,\, l,\, m,\, n,\, o,\, p \in Z \right\},$$

and

$$B = \left\{ \begin{bmatrix} q & 0 & 0 & 0 \\ 0 & r & 0 & 0 \\ 0 & 0 & s & 0 \\ 0 & 0 & 0 & t \end{bmatrix} : q,\, r,\, s,\, t \in Z \right\}.$$

The centralizer of a ($C_A(a)$) consists of all elements in A that commute with a (i.e., $a^{'}a = aa^{'}$ for all $a^{'}$ in $C_A(a)$). Since elements in B have a zero in the bottom left corner, they cannot commute with a. Let

$$a = \begin{bmatrix} 5 & 7 & 2 & 4 \\ 3 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 4 \end{bmatrix} \in A,\ y = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \in B \setminus C_A(a)$$

where $ay \neq ya$. We can find other such matrices like

$$\begin{bmatrix} 5 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 6 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

and so on from $B \setminus C_A(a)$. This ensures that $B \setminus C_A(a)$ is non-empty.

6. Conclusion

In this paper, a key exchange protocol based on *DLPFP* under matrix multiplication is proposed. Additionally, the protocol's complexity and security are examined. Then, based on *DLPFP*, we have also suggested an ElGamal cryptosystem for SHI in healthcare systems with improved security.

Acknowledgment

The authors are thankful to the reviewers and editorial members for their valuable suggestions and constructive comments.

Conflict of interest

The authors declare that there is no conflict of interest.

References

[1] Aljamaly KT, Ajeena RK. The KR-elliptic curve public key cryptosystem. *Journal of Physics: Conference Series*. 2021; 1879(3): 032046. Available from: https://dx.doi.org/10.1088/1742-6596/1879/3/032046.

[2] Eftekhari M. A Diffie-Hellman key exchange protocol using matrices over noncommutative rings. *Groups Complexity Cryptology*. 2012; 4(1): 167-176. Available from: https://doi.org/10.1515/gcc-2012-0001.

[3] Kumar S, Kumar S, Mittal G, Dharminder D, Narain S. Non-singular transformation based encryption scheme. *International Journal of Mathematical Sciences and Computing*. 2021; 7(3): 32-40. Available from: https://doi.org/10.5815/ijmsc.2021.03.04.

[4] Kryvyi SL, Opanasenko VN, Grinenko EA, Nortman YA. Symmetric information exchange system based on ring isomorphism. *Cybernetics and Systems Analysis*. 2022; 58(5): 671-682. Available from: https://doi.org/10.1007/s10559-022-00500-y.

[5] Gupta SC, Sanghi M. On an efficient RSA public key encryption scheme. *Malaya Journal of Matematik*. 2020; 8(3): 1138-1141. Available from: https://doi.org/10.26637/MJM0803/0069.

[6] Jalaja V, Anjaneyulu GS, Mohan LN. New digital signature scheme on non-commutative rings using double conjugacy. *Journal of Integrated Science and Technology*. 2023; 11(2): 471.

[7] Nivetha S, Chandramouleeswaran M. Semiring actions for multiple key sharing in public key cryptography. *Advances in Mathematics: Scientific Journal*. 2020; 9(3): 1271-1279. Available from: https://doi.org/10.37418/amsj.9.3.71.

[8] Muanalifah A, Sergeev S. Modifying the tropical version of stickel's key exchange protocol. *Applications of Mathematics*. 2020; 65(6): 727-753. Available from: https://doi.org/10.21136/AM.2020.0325-19.

[9] Pan J, Qian C, Ringerud M. Signed (group) diffie-hellman key exchange with tight security. *Journal of Cryptology*. 2022; 35(4): 26. Available from: https://doi.org/10.1007/s00145-022-09438-y.

[10] Roman'kov V. An improvement of the Diffie-Hellman noncommutative protocol. *Designs, Codes and Cryptography*. 2022; 90(1): 139-153. Available from: https://doi.org/10.1007/s10623-021-00969-2.

[11] Kanagala P. An improvement of the Diffie-Hellman noncommutative protocol. *Optik*. 2023; 272: 170252. Available from: https://doi.org/10.1016/j.ijleo.2022.170252.

[12] Koundinya AK, Gautham SK. Two-layer encryption based on paillier and elgamal cryptosystem for privacy violation. *International Journal of Wireless and Microwave Technologies*. 2021; 11(3): 9-15. Available from: https://doi.org/10.5815/ijwmt.2021.03.02.

[13] Kim SR, Kyung R. Study on modified public key cryptosystem based on elgamal and cramer-shoup cryptosystems. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference*. Las Vegas, NV, USA: IEEE; 2023. p.280-284. Available from: https://doi.org/10.1109/CCWC57344.2023.10099297.

[14] Omran EH, Al-Janabi RJ. Modified elgamal algorithm using three paring functions. In *Next Generation of Internet of Things: Proceedings of ICNGIoT*. Singapore: Springer Nature; 2022. p.405-413. Available from: https://doi.org/10.1007/978-981-19-1412-6_35.

[15] Liu Z, Gong J, Ma Y, Niu Y, Wang B. Forward and backward secure updatable ElGamal encryption scheme for cloud storage. *Journal of Systems Architecture*. 2023; 141: 102926. Available from: https://doi.org/10.1016/j.sysarc.2023.102926.

[16] Annamalai C, Vijayakumaran C, Ponnusamy V, Kim H. Optimal ELGamal encryption with hybrid deep-learning-based classification on secure internet of things environment. *Sensors*. 2023; 23(12): 5596. Available from: https://doi.org/10.3390/s23125596.

[17] Kanwal S, Inam S, Ali R, Cheikhrouhou O, Koubaa A. Lightweight noncommutative key exchange protocol for IoT environments. *Frontiers in Environmental Science*. 2022; 10: 996296. Available from: https://doi.org/10.3389/fenvs.2022.996296.

[18] Seyhan K, Nguyen TN, Akleylek S, Cengiz K, Islam SH. Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security. *Journal of Information Security and Applications*. 2021; 58: 102788. Available from: https://doi.org/10.1016/j.jisa.2021.102788.

[19] Mohit K, Hritu R, Nisha C, Sukhpal SG. Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. *Internet of Things and Cyber-Physical Systems*. 2023; 3: 309-322. Available from: https://doi.org/10.1016/j.iotcps.2023.05.006.

[20] Pathak A. An approach for secure data exchange in medical field using block chain. *Turkish Journal of Computer and Mathematics Education*. 2021; 12(7): 915-921.

[21] Al-Zubaidie M. Implication of lightweight and robust hash function to support key exchange in health sensor networks. *Symmetry*. 2023; 15(1): 152. Available from: https://doi.org/10.3390/sym15010152.

[22] Prabhu AJ, Rajesh DH. Authentication of WSN for secured medical data transmission using diffie hellman algorithm. *Computer Systems Science and Engineering*. 2023; 45(3): 2363-2376. Available from: https://doi.org/10.32604/csse.2023.028089.

[23] Zhan Y, Xuan Z. Medical record encryption storage system based on internet of things. *Wireless Communications and Mobile Computing*. 2021; 2021: 1-9. Available from: https://doi.org/10.1155/2021/2109267.

[24] Lu Y, Zhao D. A chaotic-map-based password-authenticated key exchange protocol for telecare medicine information systems. *Security and Communication Networks*. 2021; 2021: 1-8. Available from: https://doi.org/10.1155/2021/7568538.

[25] Lizama-Perez LA. Non-invertible key exchange protocol. *SN Applied Sciences*. 2020; 2(6): 1083. Available from: https://doi.org/10.1007/s42452-020-2791-3.

[26] Micheli G. Cryptanalysis of a non-commutative key exchange protocol. *Advances in Mathematics of Communications*. 2013; 9: 247-253. Available from: https://doi.org/10.48550/arXiv.1306.5326.

[27] Kahrobaei D, Koupparis C, Shpilrain V. Public key exchange using matrices over group rings. *Groups-Complexity-Cryptology*. 2013; 5(1): 97-115. Available from: https://doi.org/10.1515/gcc-2013-0007.

[28] Inam S, Kanwal S, Ali R. A new encryption scheme based on groupring. *Contemporary Mathematics*. 2021; 2(2): 103-112. Available from: https://doi.org/10.37256/cm.222021611.

[29] Eftekhari M. Cryptanalysis of some protocols using matrices over group rings. In: Joye M, Nitaj A. (eds.) *Progress in Cryptology-AFRICACRYPT 2017*. Cham: Springer International Publishing; 2017. p.223-229. Available from: https://doi.org/10.1007/978-3-319-57339-7_13.

[30] Gupta I, Pandey A, Dubey MK. A key exchange protocol using matrices over group ring. *Asian-European Journal of Mathematics*. 2019; 12(5): 1950075. Available from: https://doi.org/10.1142/S179355711950075X.

[31] Pandey A, Gupta I, Singh DK. On the security of DLCSP over $GL_n(F_q[S_r])$. *Applicable Algebra in Engineering, Communication and Computing*. 2023; 34(4): 619-628. Available from: https://doi.org/10.1007/s00200-021-00523-6.

[32] Sharma K, Agrawal A, Pandey D, Khan R, Dinkar SK. RSA based encryption approach for preserving confidentiality of big data. *Journal of King Saud University-Computer and Information Sciences*. 2022; 34(5): 2088-2097. Available from: https://doi.org/10.1016/j.jksuci.2019.10.006.

[33] Ezhilmaran D, Muthukumaran V. Key exchange protocol using decomposition problem in near-ring. *Gazi University Journal of Science*. 2016; 29(1): 123-127.

[34] Chowdhury KR, Sultana A, Mitra NK, Khan AK. Some structural properties of semirings. *Annals of Pure and Applied Mathematics*. 2014; 5(2): 158-167.

[35] Shpilrain V, Ushakov A. A new key exchange protocol based on the decomposition problem. *Algebraic Methods in Cryptography, Contemporary Mathematics*. 2006; 418: 161-167. Available from: https://doi.org/10.48550/arXiv.math/0512140.

[36] Shpilrain V. Cryptanalysis of Stickel's key exchange scheme. In: Hirsch EA, Razborov AA, Semenov A, Slissenko A. (eds.) *Computer Science-Theory and Applications*. Berlin, Heidelberg: Springer; 2008. p.283-288.

[37] Diffie W, Hellman ME. New directions in cryptography. In: Rebecca S. (ed.) *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*. New York, NY, United States: ACM; 2022. p.365-390. Available from: https://doi.org/10.1145/3549993.3550007.