Malaysian Journal of Mathematical Sciences 19(2): 553–569 (2025)
https://doi.org/10.47836/mjms.19.2.10

Malaysian Journal of Mathematical Sciences

Journal homepage: https://mjms.upm.edu.my

Cryptographic Undeniable Signature System Using DLCSFP Over Semiring

Sethupathi, S.[1] and Manimaran, A.*[1]

[1]*Department of Mathematics, School of Advanced Sciences, Vellore Institute of Technology, Vellore, India*

E-mail: marans2011@gmail.com
**Corresponding author*

Received: 9 August 2024
Accepted: 6 January 2025

Abstract

Chaum and Van first introduced the Undeniable Signature Scheme (USS) in 1989. A significant advantage of the USS scheme is that the signer participates in the verification process. In this study, we present the Discrete Logarithm Conjugacy Search Factor Problem (DLCSFP) and provide an evaluation of its security and complexity. We then propose an undeniable signature method based on DLCSFP and evaluate the security and complexity of this new scheme.

Keywords: semiring; conjugacy search problem; discrete logarithm problem; factor problem; undeniable signature; Hash function.

1 Introduction

Authentication is essential for guaranteeing the integrity and validity of a message because traditional signatures can be abused. The Message Authentication Code (MAC) is proposed to address this issue, using a message and a secret key as inputs and an authentication code as output. However, MAC's fail to meet the properties of non-repudiation and the property of being publicly verifiable [13]. A signer must also evaluate and retain a secret key and the code corresponding to each recipient if they wishes to interact with numerous recipients, which is laborious work. In 1976, Diffie and Hellman [5] proposed the concept of a digital signature to circumvent these restrictions. Several digital signature systems, including the ElGamal Signature Scheme, Digital Signature Algorithm (DSA) [23], were proposed during the same period as the digital signature scheme based on RSA in [20]. All these digital signature techniques have the attribute of global verifiability and it isn't always desirable. Undeniable signatures scheme introduced by David Chaum and Hans van Antwerpen, are a type of digital signature that requires the signer's cooperation for verification [3]. The security of the USS depends on the DLP's difficulty. The signer's cooperation is required during the verification step in undeniable signatures, and the signer cannot refute the signature's authenticity. USS include a disavowal procedure when a recipient receives a signature that is not valid.

The recipient can readily determine the cause of an unacceptable signature using the disavowal protocol, such as whether the signature is valid or not, owing to due to fraudulence or the signatory's failure to comply effectively in the verification process. Following Chaum and Antwerpen's DLP system, few undeniable signature schemes have been put forward, whose safety depends on various mathematical problems such as the Integer Factorization Problem (IFP) [8], the Conjugacy Search Problem (CSP) [25], the Elliptic Curve Discrete Logarithm Problem (ECDLP) [4] and so on.

Kahrobaei and Khan [12] proposes a non-commutative key exchange scheme extending the ElGamal Cipher to polycyclic groups. It identifies suitable group criteria for secure cryptosystems and analyzes the complexity of related decision problems. Sakalauskas et al. [21] proposes a key agreement protocol based on infinite non-commutative group presentation and representation levels. It leverages the CSP and a modified matrix-based Discrete Logarithm Problem (DLP) for security. The approach prevents cryptanalysis by avoiding CSP-to-DP reduction and transforms the Word Equivalence Problem (WEP) to the representation level, eliminating group complexity restrictions.

Eftekhari [6] presents a key exchange protocol relying on the hardness of discrete logarithms, with exponentiation concealed by conjugation. A platform-dependent cryptanalysis is provided, and a matrix group over a noncommutative ring is proposed for enhanced security. Gupta et al. [11], introduces a key exchange protocol in a non-commutative semigroup over a group ring, relying on the hardness of the Factorization with Discrete Logarithm Problem (FDLP). It includes security and complexity analysis and introduces an ElGamal cryptosystem based on FDLP using invertible matrices over group rings.

Muthukumaran [17] proposes a new approach to draft a key exchange protocol over a near-ring whose safety depends upon the mathematical problems over FP. This study [27] models the discrete logarithmic problem using non-commutative semigroup matrices over a semiring, and proposes a discrete key transfer protocol based on factorial problem (DLPFP) difficulty. Sensitive Health Information (SHI) in healthcare systems is encrypted using an ElGamal cryptosystem, and the protocol's security and complexity are examined. Tahat et al. [24] an efficient self-certified multi-proxy signature scheme with message recovery based on an elliptic curve discrete logarithm

problem is proposed. Based on the hardness of the word problem in a group, the public key cryptosystem is investigated in [9]. In this [22] work, we propose a USS based on DLFP over the semiring. We also illustrate the suggested USS and its use in Mobile Edge Computing (MEC). Secure digital signatures can benefit from certificateless cryptography's ability to improve security by eliminating certificates and resolving key management concerns. On the other hand, a public key replacement attack can be used to exploit a flaw in a suggested scheme [26].

The GGH-MKA (Goldreich-Goldwasser-Halevi) lattice-based encryption scheme has been strengthened through prior studies that established clear and rigorous rules for generating secure private and public keys, significantly boosting its security and reliability [14].

Beaula et al. [2] investigation enhances data security by using graph theory techniques like (S_g, C_3)-multi-decomposition and anti-magic decomposed labeling to encrypt and decrypt 8-character alphanumeric strings.

A new digital signature algorithm is designed [1], which proves that if an attacker tries to get the public and private keys, then an exponential time is needed as Table 1.

Table 1: Comparison table between USS and DSS.

Feature	USS	DSS
Non-repudiation	provides non-repudiation	also ensures non-repudiation
Key-dependency	typically depends on a secret key	employs a public-private key pair
Key-management	requires effective key management	entails secure management of key pairs
Algorithm type	Commonly uses hash functions from cryptography	utillizes asymmetric cryptography
Verification process	Asking the signer to disclose the secret key could be one way to verify	verification relies on the public key
Flexibility	might provide greater design and execution flexibility	standardized compatibility across various systems

In this study, we define the DLCSFP, which is a mixture of DLP, CSP, and FP over a non-abelian group. Utilizing the safety and assurance settings, the complexity of brute force attacks is also thoroughly examined. We provide an undeniable signature scheme whose security in a non-abelian group over semiring depends on the DLCSFP's hardness. The security analysis and the complexity analysis of the suggested scheme are also given. The paper is organized as outlined below.

In Section 2, this paper provides the preliminaries and discuss the combination of DLP, CSP, and FP necessary for understanding the work. Section 3 discusses a non-abelian group over semiring based signature system. In Section 4, it analyzes the proposed scheme's security and complexity. Finally, Section 5, ends with a conclusion.

Table 2 is a list of the concepts utilized in the paper.

Table 2: List of notation.

Notation	Description
$\mathbb{S}_{\mathbb{R}}$	Semiring
$Z_p \setminus \{0,1\}$	Ring of integer modular and remove 1
H	Commutative semiring
H_1,H_2	Subsemiring
$C_G(g)$	Centralizer of g
F	Non commutative group
L	Commutative subgroup
$t(m_1)$	Hash function
$(0,1)^*$	Set of all finite-length strings of 0s and 1s, including the empty string

Abbreviations

In this paper, the following list of abbreviations in Table 3 is used.

Table 3: **List of Abbreviations**

Abbreviations	Name
CDL	Conjugacy Search Problem and Discrete Logarithm Problem
CSP	Conjugacy Search Problem
FP	Factor Problem
DH	Diffie Hellman
DLCSP	Discrete Logarithm Conjugacy Search Problem
DLCSFP	Discrete Logarithm Conjugacy Search Factor Problem
DLFP	Discrete Logarithmic Factor Problem
DLP	Discrete Logarithm Problem
DP	Disavowal protocol
DSA	Digital Signature Algorithm
DS	Digital Signature
DSS	Digital Signature Scheme
USS	Undeniable Signature Scheme
VP	Verification Protocol

2 Preliminaries

In this section, we define the semiring, CSP, DLP, and FP for more details refer [19, 18].

Definition 2.1 (Semiring)**.** ($\mathbb{S}_{\mathbb{R}}$)[19] *A nonempty set called a semiring* ($\mathbb{S}_{\mathbb{R}}$) *with addition and multiplication defined as,*

1. *The commutative monoid* $(\mathbb{S}_{\mathbb{R}}, +)$ *has identity element 0.*
2. *A monoid with identity element 1 is represented by* $(\mathbb{S}_{\mathbb{R}}, \cdot)$.
3. *Multiplication is distributive over addition from both sides.*
4. *For every* r *in* $\mathbb{S}_{\mathbb{R}}, 0 \cdot r = 0 = r \cdot 0$.

Definition 2.2 (Conjugacy Search Problem). [18] *In a non-commutative group* $(H, \cdot)$*, for a given a,b* $\in H$*, the conjugacy search problem is to find* $x \in H$ *such that* $a = x^{-1} \cdot b \cdot x$*.*

Definition 2.3 (Discrete Logarithm Problem(DLP)). [15] *Let* p *be a prime and given an element* $\beta \in Z_p$ *where* Z_p *is a cyclic group of order* $p-1$ *generated by* α*, find an integer,* $0 \leq t \leq p-1$ *such that* $\alpha^t \equiv \beta \pmod{p}$*.*

Definition 2.4 (Factor Problem). [16] *Let* x *be an arbitrary element in non-commutative semiring* H*, and let* H_1 *and* H_2 *be two subsemirings in* H*. Factor problem* (FP) *is defined as finding any two elements* $x_1 \in H_1, x_2 \in H_2$ *such that* $l = x_1 x_2$*.*

Definition 2.5 (Hash function). [13] *A hash function (with output length* ℓ*) is a pair of probabilistic polynomial-time algorithms* (Gen, H) *satisfying the following:*

- *Gen is a probabilistic algorithm that takes as input a security parameter* 1^n *and outputs a key* s*. We assume that* 1^n *is implicit in* s*.*
- H *takes as input a key* s *and a string* $x \in \{0,1\}^*$ *and outputs a string* $H_s(x) \in \{0,1\}^{\ell(n)}$ *(where* n *is the value of the security parameter implicit in* s*).*

Definition 2.6. *Let* F *be a non-commutative group and* H *be a commutative subgroup of* F*. Let* $y_1' \in F$ *such that* $y_1' = x z_1^{i_1} z_2^{i_2} x^{-1}$ *where* x*,*z_1*and* $z_2 \in F$*,* $i_1, i_2 \in Z_p \setminus \{0,1\}$ *and* p *is a prime. The DLCSFP is to find* x*,*i_1*,* i_2 *where* y_1'*,*z_1 *and* z_2 *are public parameters.*

The security level that the creator of the cryptosystem wants is expressed in H and p, as defined in Definitions 2.1, 2.2, 2.3, 2.4, 2.5 and 2.6.

3 Undeniable Signature Scheme based on Semiring

We propose a new undeniable signature method in this part, whose security is based on the DLCSFP introduced in Definition 2.6. The following is a description of the signature scheme:

Set-Up:
Let $F = M_{n\times n}(S_R)$ have an abelian subgroup L.
The definition of a hash function t is $(0,1)^* \to F \setminus L$.

Key-Gen:
Let $P = X A_1^{a_1} A_2^{a_2} X^{-1}$ and $A_1, A_2 \in F \setminus L$, where $X \in N$ and $a_1, a_2 \in Z_p \setminus \{0,1\}$. The private key of the signer is $SK = (X, a_1, a_2, N, A_2)$ and the public key is $PK = (P, A_1)$.

Sign-Gen:
A message $m_1 \in (0,1)^*$ has

$$S = f(t(m_1))^{a_1 a_2} f^{-1} = X A_1^{a_1} A_2^{a_2} (t(m_1))^{a_1 a_2} A_2^{a_2^{-1}} A_1^{a_1^{-1}} X^{-1},$$

as signature, where $f = A_1^{a_1} A_2^{a_2}$ and $t(m_1) \in H \setminus L$.

Verification protocol:
To verify the signature S's authenticity, a verifier performs the following steps:

Step 1: After obtaining the message m's signature, S computes $C = (UP^{-1}SPU^{-1})^{b_1 b_2}$, which C sends to the signer. A random matrix $U \in L$ and a random integer $b_1, b_2 \in Z_p \setminus \{0, 1\}$ are selected by the verifier.

Step 2: $Q = (X^{-1}CX)^{a_1^{-1} a_2^{-1}}$ is computed by the signer and sent to the verifier.

Step 3: To verify whether $Q = Q_1$ or not, calculate $Q_1 = U(t(m_1))^{b_1 b_2} U^{-1}$ and determine accordingly.

Step 4: If the signature is true, $Q = Q_1$. Now consider the verification protocol's soundness and completeness.

The verification protocol's completeness and soundness:
The following theorem is used to confirm the verification protocol's soundness and completeness.

Completeness:
If the signer and the verifier follow the protocol's guidelines, the verification procedure is considered successful.

Theorem 3.1. *For any matrices $A_1, A_2 \in F \setminus L$, $X, U \in L$, $a_1, a_2 \in Z_p \setminus \{0, 1\}$, $t(m_1) \in H \setminus L$ is a hash function, if $Q = (X^{-1}CX)^{a_2^{-1} a_1^{-1}}$ and $Q_1 = U(t(m_1))^{b_1 b_2} U^{-1}$, then the verification protocol is complete $i.e, Q = Q_1$.*

Proof. The private key (X, a_1, a_2, N, A_2) is used by the signer to compute $Q = (X^{-1}CX)^{a_2^{-1} a_1^{-1}}$. The verifier then computes $C = (UP^{-1}SPU^{-1})^{b_1 b_2}$, obtains the signature S in m, and returns it to the signer. Following the formula below, the verifier states that $Q = Q_1$.

$$
\begin{aligned}
Q &= (X^{-1}CX)^{a_2^{-1} a_1^{-1}} \\
&= (X^{-1}C^{a_2^{-1} a_1^{-1}}X) \\
&= X^{-1}\left\{(UP^{-1}SPU^{-1})^{b_1 b_2}\right\}^{a_2^{-1} a_1^{-1}} X \\
&= X^{-1}\Big\{(U(XA_2^{a_2^{-1}} A_1^{a_1^{-1}} X^{-1})(XA_1^{a_1} A_2^{a_2} t(m_1)^{a_1 a_2} A_2^{a_2^{-1}} A_1^{a_1^{-1}} X^{-1}) \\
&\quad (XA_1^{a_1} A_2^{a_2} X^{-1})U^{-1})^{b_1 b_2}\Big\}^{a_2^{-1} a_1^{-1}} X \\
&= X^{-1}\left\{(U(Xt(m_1)^{a_1 a_2})X^{-1})^{b_1 b_2}\right\}^{a_2^{-1} a_1^{-1}} U^{-1} X \\
&= X^{-1}\left\{XUt(m_1)^{a_1 a_2 a_2^{-1} a_1^{-1} b_1 b_2} U^{-1} X^{-1}\right\} X \\
&= Ut(m_1)^{b_1 b_2} U^{-1} = Q_1.
\end{aligned}
$$

As a result, after receiving Q_1, the verifier checks to see if $Q = Q_1$. If it does, he accepts the signature. □

Soundness:
If a dishonest signer cannot persuade the verifier to accept an invalid signature, the verification protocol is considered to be sound.

Theorem 3.2. *Less than the maximum of* $\left(\frac{1}{dt}, \frac{1}{e-d}\right)$*, where* d *is the order of* L *and* e *is the order of* F*, may a dishonest signer expect the verifier to accept an invalid signature.*

Proof. The dishonest signer will attempt to extract the pair (U, b_1, b_2) to compute Q so that $Q = Q_1$, or he will choose an element $\bar{Q} \in F \setminus L$ so that $\bar{Q} = Q_1$, after receiving $C = (UP^{-1}SPU{-}1)^{b_1 b_2}$ from the verifier. The probability of selecting the correct pair (U, b_1, b_2) in the first scenario is not larger than $\frac{1}{dt}$, where $U \in L$ and $b_1, b_2 \in Z_p \setminus \{0, 1\}$. The likelihood in the second situation is not more than $\frac{1}{e-d}$. □

3.1 Disavowal protocol

When the verifier receives an invalid signature, the disavowal protocol comes into play. In the following two scenarios, the signature should be invalid:

(a) At the verification step, the signer is dishonest.

(b) The message has been forged in an unauthorized way.

The verifier can determine whether the foregoing situations have occurred using the disavowal process.

The verifier moves on to the next round if it determines that $Q = Q_1$, or that $Q = t(m_1)^{b_1 b_2} U^{-1}$. The validation procedure is involving new random elements in $U_1 \in L$ and $b_3, b_4 \in Z_p \setminus \{0, 1\}$.

If the verifier calculates $C_1 = (U_1 PSP^{-1} U_1^{-1})$ and sends it to the signer, the verifier then notes that $Q_2 = U_1(t(m_1))^{b_1 b_2} U_1^{-1}$ upon receiving $Q_3 = (X^{-1} C_1 X)^{a_2^{-1} a_1^{-1}}$ from the signer, and comes to the conclusion that $t(m_1)$ is fabricated if and only if $UQ_2^{b_1 b_2} U^{-1} = U_1 Q^{b_3 b_4} U_1^{-1}$.

Disavowal protocol's completeness and soundness:
The following theorems are employed to confirm the accuracy and validity of the disavowal process.

Completeness:
If the verifier consistently determines that the signature on message m_1 is fraudulent, the disavowal process will be halted.

Theorem 3.3. *For any matrices* $A_1, A_2 \in F \setminus L$*,* $X, U \in L$ *and* $a_1, a_2 \in Z_p \setminus \{0, 1\}$ *if the verifier consistently gets,*

$$S \neq X A_1^{a_1} A_2^{a_2} (t(m_1))^{a_1 a_2} A_2^{a_2^{-1}} A_2^{a_1^{-1}} X^{-1},$$

then the disavowal protocol is complete, i.e.,

$$UQ_3^{b_1 b_2} U^{-1} = U_1 Q_4^{b_3 b_4} U^{-1}. \tag{1}$$

Proof. Let $A_1, A_2 \in F$, $X \in L$ and $a_1, a_2 \in Z_p \setminus \{0, 1\}$, we begin by calculating the left hand side

of (1),

$$\begin{aligned} UQ_3^{b_1b_2}R^{-1} &= U(X^{-1}C_1X)^{b_1b_2a_2^{-1}a_1^{-1}}U^{-1} \\ &= U(X^{-1}(U_1(XA_2^{a_2^{-1}}A_1^{a_1^{-1}}X^{-1})(XA_1^{a_1}A_2^{a_2}(t(m_1))^{a_1a_2}A_2^{a_2^{-1}}A_1^{a_1^{-1}}X^{-1}) \\ &\quad (XA_1^{a_1}A_2^{a_2}X^{-1}U_1^{-1})^{b_3b_4}X)^{b_1b_2a_2^{-1}a_1^{-1}}U^{-1} \\ &= U(X^{-1}(X(U_1(t(m_1))^{a_1a_2b_3b_4}U_1^{-1}))X^{-1})X)^{b_1b_2a_2^{-1}a_1^{-1}}U^{-1} \\ &= U(U_1t(m_1)^{a_1a_2a_2^{-1}a_1^{-1}b_3b_4}U_1^{-1})^{b_1b_2}U^{-1} \\ &= UU_1t(m_1)^{b_1b_2b_3b_4}U_1^{-1}U^{-1}. \end{aligned} \tag{2}$$

Now calculating the other side in a similar way,

$$U_1Q_4^{b_3b_4}U^{-1} = UU_1t(m_1)^{b_1b_2b_3b_4}U_1^{-1}U^{-1}. \tag{3}$$

From (1) and (2), we get,

$$UQ_3^{b_1b_2}U^{-1} = U_1Q_4^{b_3b_4}U^{-1}. \tag{4}$$

Therefore the disavowal protocol is complete. □

Soundness:
A disavowal protocol is considered valid if a dishonest signer is unable to persuade the verifier to recognize a legitimate signature as a forged one.

Theorem 3.4. *The likelihood that the dishonest signer will be successful in persuading the verifier to accept a legitimate signature as a fraudulent signature is not larger than t maximum of $\left(\frac{1}{dp}, \frac{1}{e-d}\right)$ where d is the order of F and e is the order of L.*

Proof. Assume,

$$S = XA_1^{a_1}A_2^{a_2}(t(m_1))^{a_1a_2}A_2^{a_2^{-1}}A_1^{a_1^{-1}}X^{-1},$$

is a legal signature for $t(m_1)$. If the following conditions are met, a dishonest signer may persuade a verifier that S is a created signature.

$$\begin{aligned} Q_3 &\neq Ut(m_1)^{b_1b_2}U^{-1}, \\ Q_4 &\neq U_1t(m_1)^{b_3b_4}U_1^{-1}. \end{aligned}$$

$$UQ_3^{b_1b_2}U^{-1} = U_1Q_4^{b_3b_4}U^{-1}. \tag{5}$$

However, if we make the assumption, we will end up with a contradiction, which is shown below. From (1), we get,

$$\begin{aligned} Q_3 &= U^{-1}(U_1Q_4^{b_3b_4}U_1^{-1})^{b_2^{-1}b_1^{-1}}U \\ &= U_1(U^{-1}Q_4^{b_2^{-1}b_1^{-1}}U)^{b_3b_4}U_1^{-1}. \end{aligned}$$

$$Q_3 = U^1K^{b_3b_4}U_1^{-1}, \quad \text{where} \quad K = U^{-1}Q_4^{b_2^{-1}b_1^{-1}}U. \tag{6}$$

The verification protocol's soundness properly shows that the probability is minimum of

$$\left(1-\frac{1}{dp},1-\frac{1}{e-d}\right).$$

For a valid signature S for F besides the valid signature for $t(m_1)$ is S. Check $t(m_1)=F$ which is intimated by,

$$XA_1^{a_1}A_2^{a_2}(t(m_1))^{a_1a_2}A_2^{a_2^{-1}}A_1^{a_1^{-1}}X^{-1}=XA_1^{a_1}A_2^{a_2}K^{a_1a_2}A_2^{a_2^{-1}}A_1^{a_1^{-1}}X^{-1},$$

with the same probability given above. It is a contradiction because,

$$t(m_1)\neq U^{-1}Q_4^{b_2^{-1}b_1^{-1}}U=K,$$

from (5) since, $Q_4 \neq Ut(m_1)^{b_1b_1}U^{-1}$. This implies that the signature S is valid on $t(m_1)$. The condition in (5) is not correct. The maximum of $\left(\frac{1}{dp},\frac{1}{e-d}\right)$ is lesser than the maximum of

$$\left(1-\left(1-\frac{1}{dp}\right),1-\left(1-\frac{1}{e-d}\right)\right).$$

□

Remark 3.1. *During the verification and disavowal protocol the hidden parameters are not revealed so, the scheme is safe and secure. The fact that the system isn't considered a zero-knowledge undeniable signature system may not mean much, however,*

$$\left(1-\frac{1}{dp},1-\frac{1}{e-d}\right).$$

4 Analysis of the Proposed Undeniable Signature Method's Complexity and Security

The ensuing sections address the intricacy and safety of the suggested incontrovertible signature method.

4.1 Security analysis

Data Forgery:
The attacker in this instance aims to substitute the false message m_1' for the real message m_1. The adversary will do this by either attempting to get the signer's private keys or by discovering a message $m_1' \neq m_1$ such that $h(m_1')=h(m_1)$. The adversary will be given the task of solving the DLCSFP in the first scenario, which is computationally infeasible for particular values as stated in Definition 2.6. If the hash function creates the scheme as pre-image resistant, the second scenario will also be computationally infeasible.

Hidden:
We make improvements in the security by concealing the subgroup L. For generating the key in the undeniable signature scheme, the matrices A_1, A_2 and X are selected from F\L. When the

adversary tries to decrypt, he does not know because L is hidden. These two enhancements are explained in [7].

Existential Forgery:
In this situation [23], an adversary will attempt to produce a valid signature for at least one communication. This can be achieved through one of three methods:

(i) **Existential forging through a well-known messaging attack:**
Let S represent the totality of the message-related signatures. Suppose a hacker decides to forge the signature using (m_1, s) in S. In order to make $h(m_1') = h(m_1)$ in this scenario, suppose the adversary will attempt to locate a $m_1' \neq m_1$. However, the method is secure against this circumstance because of the employment of a second pre-image resistant mechanism. The attacker must compute Q_4 even if $h(m_1) = h(m_1')$ and (m_1', s) are able to establish a valid signature $m_1' \neq m_1$. But it's not possible because of DLCSP and $FP's$ difficulties.

(ii) **Existential fraud with a targeted message attack:**
Assume that a set of S message signature combinations is possessed by your opponent. The opponent is going to try to interpret two messages. A valid signature (m_1', S) and (m_1', m_1) with hash values that are not equal, i.e. $h(m_1') \neq h(m_1)$. The scheme is protected against this attack because it employs a hash function that resists collisions. Permit the opponent to obtain a message $m \neq m'$ with the following properties: (m_1', S) is a legal signature, $(h(m_1) = h(m_1')$. The adversary will then confront the difficulty of solving the DLCSP as in [10] and in this paper, the inclusion of parameter a_2 and the matrix A_2 becomes another DLCSP which gives double security against Q_4 computation during the verification process. $A_1^{a_1} A_2$ is considered a hard problem in [11]. Given that it is a computationally difficult challenge, as indicated in Section 3, the DLCSFP is safe against existential forging via selected message attacks.

(iii) **Existential forging by complete break:**
An attacker attempting to counterfeit the signature in this instance is not aware of the message-signature association. In order to accomplish this, the adversary will attempt to construct an invalid signature during communication. However, the technique is secure against this attack due to the employment of a hash function that is pre-image resistant. Theorem 3.4 investigates the possibility that the verifier will accept a false signature. This means that existential forgery cannot penetrate the system, and the previous discussion can be summarized as follows.

Theorem 4.1. *The DLCSFP problem can be solved if there exists an existential forgery.*

Theorem 4.2. *The likelihood that a fraud signature is accepted by the verifier is at most* $\frac{1}{|\ F \setminus L\ |}$, *where F\L is the cardinality of* $|\ F \setminus L\ |$.

Proof. Let us say someone tries to falsify the signature. The enemy will take the following measures to accomplish this. The opponent will select X' in N and $a_1', a_2' \in Z_p \setminus \{0, 1\}$ before calculating,

$$S' = X' A_1^{a_1'} A_2^{a_2'} t(m_1)^{a_1' a_2'} A_2^{a_2'^{-1}} A_1^{a_1'^{-1}} X'^{-1},$$

and sending $(t(m_1), S')$ to the person who verifies.

The signatory receives $C' = RP^{-1} S'^{b_1 b_2} PR^{-1}$ and C' after the verifier receives $(t(m_1), S')$ and certifies that it is a valid signature. When the adversary intercepts in the middle, they calculate $Q' = (X'^{-1} C' X')^{a_2'^{-1} a_1'^{-1}}$.

The adversary subsequently sends it to the verifier. If there is a tie, the opponent forges the signature to win. The verifier analyses $Q_1' = Rh(m_1)^{b_1 b_2} R^{-1}$ and compares it with $Q'. = Q_1'$ in order to confirm the signature. To keep this equilibrium in place and ensure that $Q' = Q_1'$, $Q', Q_1' \in F \setminus L$, the adversary will select the parameters in the first phase. Following are the calculations for the likelihood that $Q' = Q_1'$: Let e and d represent F and L's respective cardinality.

The amount of ways to obtain Q', Q_1' as (Q', Q') or (Q_1', Q_1') from $F \setminus L$, i.e., $Q' = Q_1'$, is ed. As a result, a large proportion of cases are $(e - d)$. The amount of ways to select (Q', Q_1') out of $F \setminus L \times F \setminus L$ are $(e-d)^2$. As a result, the likelihood of the person who verifies accepting a forged sign is,

$$\frac{e-d}{(e-d)^2} < \frac{1}{(e-d)} = \frac{1}{F \setminus L}.$$

Selecting the size of the abelian subgroup L to preserve $F \setminus L$ variability is crucial. □

4.2 Complexity analysis

Using the parameters outlined in Definition 2.6, the following calculates the total number of operations required for key generation, signature generation, verification, and the disavowal protocol in the proposed undeniable signature system.

Required number of operations in generation of key:
We must calculate $P = X A_1^{a_1} A_2^{a_2} X^{-1}$ for key generation, where $A_1, A_2 \in F \setminus L$, $a_1, a_2 \in Z_p \setminus \{0, 1\}$. The matrices X, A_1 and A_2 are of order n and are taken over semiring $(\mathbb{S}_{\mathbb{R}})$. Multiplying two matrices of order n requires no more than $O(n^3)$ bit operations [10]. Thus, $(2n^3 \log p)$ is the total number of operations needed to compute $A_1^{a_1}, A_2^{a_2}$ [10]. Finally, we need $3n^3$ additional procedures to calculate $X A_1^{a_1} A_2^{a_2} X^{-1}$. Thus, $n^3(2 \log p + 3)$ is the total number of operations required for key Generation, and this number is proportional to $O(n^3 \log p)$.

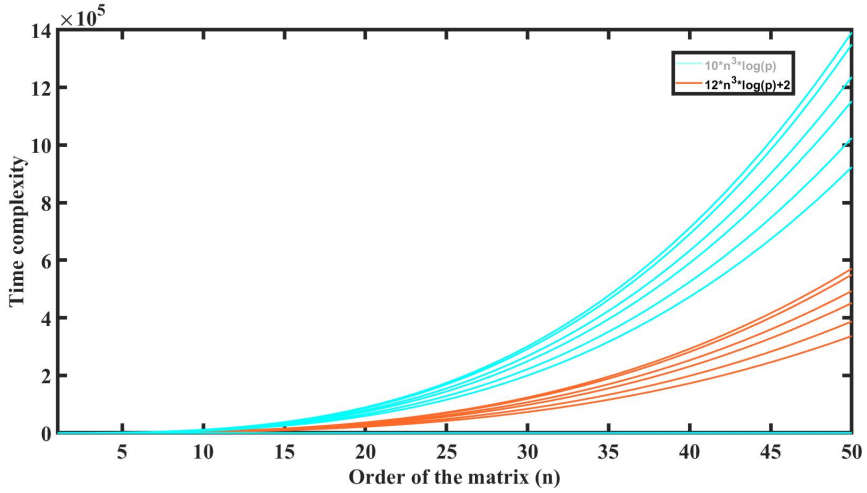

Figure 1: Comparison of the number of operations needed for Key-Generation using DLCSP and DLCSFP.

Figure 1 illustrates the temporal complexity of the key generation for the DLCSFP-based undeniable signature scheme and the DLCSP-based undeniable signature scheme, based on the values

of n. The matrix's order is shown on this graph by the x-axis. The temporal complexity of the DLCSP and DLCSFP-based techniques is plotted on the y-axis. Figure 1 illustrates the curve for fixed prime numbers with $p = 15(say)$. For various values of n, the value curves illustrate the computational complexity of key generation in the DLCSP based undeniable signature technique. For different values of x, the red curves show the temporal complexity of key generation in the DLCSFP based undeniable signature method. In contrast to the blue and red curves, it is evident that the main generation temporal complexity results in a positive slope of the curve as the matrix order increases. By analyzing the blue and red curves in the picture, it is evident that there is a small variation in the slope. The constant and coefficient factors in the time complexity of the key generation of the schemes are to blame for this. At the least, the temporal complexity is proportional to $(O(n^3 \log p))$.

Required number of operations for generation of sign:
In order to compute

$$S = XA_1^{a_1}A_2^{a_2}(t(m_1))^{a_1a_2}A_2^{a_2^{-1}}A_1^{a_1^{-1}}X^{-1}$$

is a signature on a message m_1. The number of bit operations needed to create the signature is proportional to $O(n^3 \log p)$, as we observed in the key generation phase.

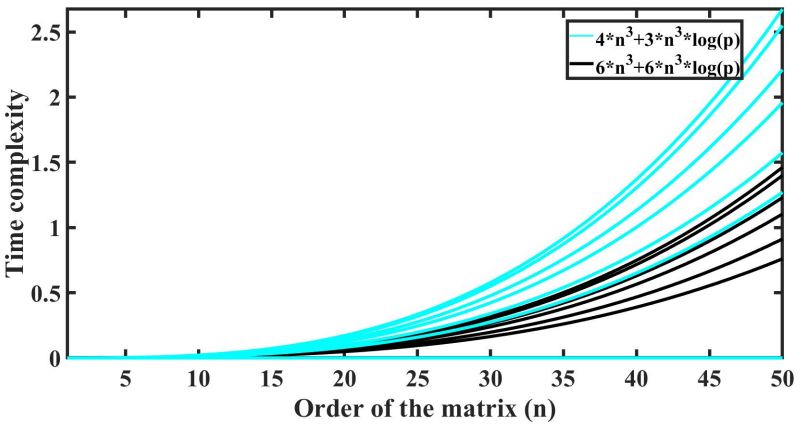

Figure 2: Comparison of the operations needed for Signature Generation using DLCSP and DLCSFP.

Figure 2 illustrates graphically the total number of processes needed for the production of a signature. Both graphs indicate that the run time is proportional to $O(n^3 \log p)$, with a slight variance in the positive slope of the curve, based on the results displayed in Figure 2. The runtime of undeniable signature systems based on DLCSP and DLCSFP is compared in Figure 2 for varying matrix sizes.

When one closely observes the divergence of the black curves and the blue curves, the relationship between (n) and temporal complexity becomes evident. The curve's positive slope can be attributed to this. The curves in the two systems are distinguished by the signature formation's coefficient terms and temporal complexity constant. These methods of unquestionable signatures have a time complexity of $(O(n^3 \log p))$.

Required number of operations in verification protocol:
To determine the activity level in the validation process, we employ the same technique as previously $5n^3 \log p$. The expression $C = (UP^{-1}SPU^{-1})^{b_1b_2}$ can be calculated by summing up all bit operations. Then, each term $Q = (X^{-1}CX)^{a_1a_2}$ and $Q_1 = (U(h(m))^{b_1b_2}U^{-1})$ will require $n^3 \log p$

operations for calculation. The verification protocol's step 4 comparison requires only one operation. As a consequence, $6n^3 \log p + 1$ bit operations are required in total for signature verification, corresponding to $O(n^3 \log p)$.

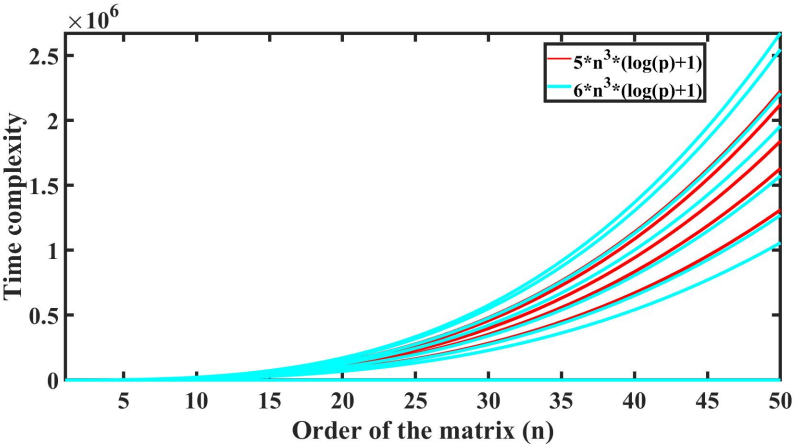

Figure 3: Comparison of the number of operations needed for verification protocols based on DLCSP and DLCSFP.

A graphical representation of the total operations required for the verification protocol is shown in Figure 3. Although the number of operations required is proportional to $O(n^3 \log p)$, it can be seen from Figure 3 that there is a positive slope. The graph shows variations in the curve. For different values of DLCSP and n, the time complexity or number of operations needed for the verification protocol of a nonrepudiation signature scheme based on DLCSFP is displayed in Figure 3. On the x-axis, the matrix (n) sequence is displayed, and on the y-axis, the number of operations needed for the nonrepudiation signature scheme verification protocol based on DLCSP and DLCSFP. Figure 3 shows the curves in blue and red for fixed values of the primary $(p = 15say)$.

The number of operations required to validate the DLCSP-based undeniable signature method is shown by the blue curves for a range of values of n. The number of operations needed to validate an undeniable signature method based on DLCSFP is represented by red curves for different values of n. When these curves are shown side by side, it is evident that the red and blue curves have positive slopes. Furthermore, the verification procedure of the DLCSFP and DLCSP based undeniable signature technique requires $(O(n^3 \log p))$ operations.

Required number of operations in disavowal protocol:
The verification protocol requires several operations of $12n^3 \log p + 2$, which is proportional to $O(n^3 \log p)$, because it has one fewer rounds than the disavowal technique.

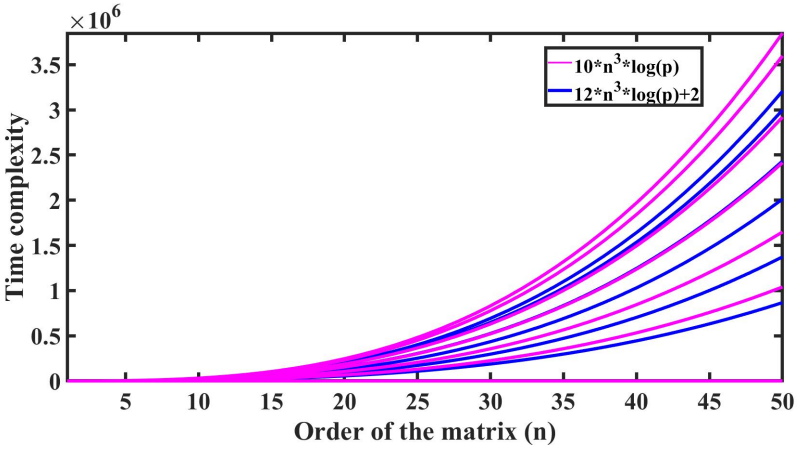

Figure 4: Comparison between the time complexity for disavowal protocol in and the proposed scheme based on DLCSP and DLCSFP.

The obtained outcome of the run time of the disavowal protocol is displayed in Figure 4. As per our result, the time complexity of [10] $(10n^3 \log p + 2)$ and our scheme $(12n^3 \log p + 2)$, have positive slopes with little difference. Like the previous scheme's graph, our scheme's graph shows some similarities in Figure 4.

Figure 4 shows the temporal complexity of the DLCSFP based undeniable signature scheme and the disavowal process of the DLCSP based undeniable signature technique. The x-axis of the graphs shows the matrix order (n), while the y-axis indicates the time complexity of the scheme's disavowal protocol based on DLCSFP across various n values and DLCSP for a range of n values.

The graph's curves take on the appearance shown in Figure 4 when the prime p value is $15(\text{say})$. For different values of n, the blue curves illustrate the time complexity of the non-repudiation protocol for the DLCSP signature method. For different choices of the matrix's order, the time complexity of the disavowal protocol for the non-repudiation signature method based on DLCSFP is shown in the figure in magenta. It is evident from examining the two curves in Figure 4 that the term complexity rises in tandem with n, or more specifically, the matrix's complexity. The generated curves have a slope that is positive. The DLCSFP based scheme's curves and the DLCSP based scheme's curves can be compared to see that the curves slopes differ slightly.

Observing the diagram, we can see that the word complexity increases with n or the complexity of the matrix. Positive slopes are found in the resulting curves. The curves slopes clearly differ slightly when comparing the time complexity between DLCSP and DLCSFP. This difference in the positive slopes shows that the coefficient and constant terms have an impact on the number of operations needed to complete the process. In every scenario, the time issues are proportional to $O(n^3 \log p)$.

The graph's blue and magenta curves can be closely examined to determine that the undeniable signature scheme based on DLCSFP has a lower runtime than the undeniable signature strategy based on DLCSP. The advantage of the suggested protocol over the old one is that it is more efficient and requires less processes. By concealing the secret parameters X, a_1, a_2, N, and A_2 as well as the commutative subgroup, the suggested undeniable signature scheme's security is increased.

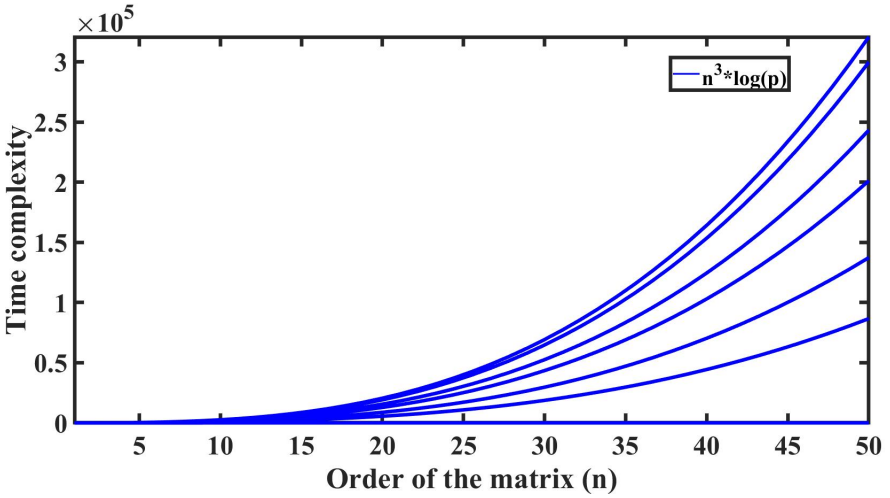

Figure 5: Number of steps required for the proposed scheme.

The matrix's order, (n), is represented by the x-axis, and its $O(n^3 \log p)$, by the y-axis. Figure 5 provides proof that the y-axis values increase in tandem with the matrix order, resulting in a positive slope curve. The graphs in Figure 1 have slightly different slopes. The order of the matrix and the number of operations required for undeniable signature scheme based on DLCSFP. Comparing the security of the proposed scheme and the scheme in [10], the proposed scheme is better and more secure than the scheme in [10].

5 Conclusion

In this paper, we introduce a novel problem called DLCSFP. We analyze its security and assess its complexity using an exhaustive search method. A USS based on the DLCSFP is proposed using a semiring as the platform, and an example is provided. The completeness and soundness of the plan are indicated by the theorems. Various kinds of attacks give the USS security. The time complexity for each step in the USS is analyzed and illustrated using graphical representations, which exhibit the same runtime as the current scheme.

Acknowledgement The authors acknowledge the support and contributions of all who assisted in the completion of this article.

Conflicts of Interest The authors declare there is no conflict of interest.

References

[1] M. Alinejad, S. Hassan Zadeh & N. Biranvand (2022). Digital signature with elliptic curves over the finite fields. *Journal of Discrete Mathematical Sciences and Cryptography*, *25*(5), 1289–1301. https://doi.org/10.1080/09720529.2020.1743503.

[2] C. Beaula, P. Venugopal & N. Sujaudeen (2024). Encryption and decryption using decomposition of complete graph $k_{3(6n+1)}$. *Malaysian Journal of Mathematical Sciences*, *18*(2), 371–397. https://doi.org/10.47836/mjms.18.2.10.

[3] D. Chaum & H. Van Antwerpen (1990). Undeniable signatures. In *Advances in Cryptology–CRYPTO'89 Proceedings 9*, volume 435 pp. 212–216. Springer, New York. https://doi.org/10.1007/0-387-34805-0_20.

[4] T. S. Chen, E. T. Hsu & Y. L. Yu (2006). A new elliptic curve undeniable signature scheme. *International Mathematical Forum*, *1*(31), 1529–1536.

[5] W. Diffie & M. E. Hellman (2022). *New Directions in Cryptography*, pp. 365–390. Association for Computing Machinery, New York. https://doi.org/10.1145/3549993.3550007.

[6] M. Eftekhari (2012). A Diffie–Hellman key exchange protocol using matrices over noncommutative rings. *Informatica*, *4*(1), 167–176. https://doi.org/10.1515/gcc-2012-0001.

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

[8] R. Gennaro, T. Rabin & H. Krawczyk (2000). RSA-based undeniable signatures. *Journal of Cryptology*, *13*, 397–416. https://doi.org/10.1007/s001450010001.

[9] N. Ghadbane (2021). On public key cryptosystem based on the word problem in a group. *Malaysian Journal of Computing and Applied Mathematics*, *4*(1), 13–16. https://doi.org/10.37231/myjcam.2021.4.1.70.

[10] N. Goel, I. Gupta, M. K. Dubey & B. K. Dass (2016). Undeniable signature scheme based over group ring. *Applicable Algebra in Engineering, Communication and Computing*, *27*, 523–535. https://doi.org/10.1007/s00200-016-0293-8.

[11] I. Gupta, A. Pandey & M. K. Dubey (2019). A key exchange protocol using matrices over group ring. *Asian-European Journal of Mathematics*, *12*(5), Article ID: 1950075. https://doi.org/10.1142/S179355711950075X.

[12] D. Kahrobaei & B. Khan (2006). Nis05-6: A non-commutative generalization of ElGamal key exchange using polycyclic groups. In *IEEE Globecom 2006*, volume 2006 pp. 1–5. Francisco. IEEE. https://doi.org/10.1109/GLOCOM.2006.290.

[13] J. Katz & Y. Lindell (2007). *Introduction to Modern Cryptography: Principles and Protocols*. CRC Press, Bora Raton, Florida.

[14] A. Mandangan, H. Kamarulhaili & M. A. Asbullah (2021). An upgrade on the key generation algorithm of the GGH-MKA lattice-based encryption scheme. *Malaysian Journal of Mathematical Sciences*, *15*(S), 25–37.

[15] A. J. Menezes, P. C. Van Oorschot & S. A. Vanstone (2018). *Handbook of Applied Cryptography*. CRC Press, Bora Raton, Florida.

[16] V. Muthukumaran & D. Ezhilmaran (2018). New key agreement protocol based on factor problem in centralizer near-ring. *Journal of Science and Arts*, *18*(2), 375–380.

[17] V. Muthukumaran, D. Ezhilmaran, I. Muchtadi-Alamsyah, R. Udhayaku-Mar & A. Manickam (2020). New public key cryptosystem based on combination of NREP and CSP in non-commutative near-ring. *Journal of Xi'an University of Architecture and Technology*, *12*(3), 4534–4539.

[18] A. G. Myasnikov, V. Shpilrain & A. Ushakov (2011). *Non-commutative Cryptography and Complexity of Group-theoretic Problems* volume 177 of *Mathematical Surveys and Monographs*. American Mathematical Society, Rhode Island.

[19] S. Nivetha, V. Thiruveni & M. Chandramouleeswaran (2019). Semiring actions for public key cryptography. *Journal of Computer and Mathematical Sciences*, *10*(1), 238–244.

[20] R. L. Rivest, A. Shamir & L. Adleman (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342.

[21] E. Sakalauskas, P. Tvarijonas & A. Raulynaitis (2007). Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level. *Informatica*, *18*(1), 115–124. https://doi.org/10.15388/Informatica.2007.167.

[22] S. Sethupathi & A. Manimaran (2024). Cryptographic signature scheme for mobile edge computing using DLFP over semiring. *Contemporary Mathematics*, *5*(2), 2353–2375. https://doi.org/10.37256/cm.5220244061.

[23] D. R. Stinson (2013). *Cryptography: Theory and Practice*. CRC Press, London second indian reprint edition.

[24] N. Tahat, A. K. Alomari, O. M. Al-Hazaimeh & M. F. Al-Jamal (2020). An efficient self-certified multi-proxy signature scheme based on elliptic curve discrete logarithm problem. *Journal of Discrete Mathematical Sciences and Cryptography*, *23*(4), 935–948. https://doi.org/10.1080/09720529.2020.1734293.

[25] T. Thomas & A. K. Lal (2008). A zero-knowledge undeniable signature scheme in non-abelian group setting. *International Journal of Network Security*, *6*(3), 265–269.

[26] M. Tian, L. Huang & W. Yang (2011). On the security of a certificateless short signature scheme. *IACR Cryptology ePrint Archive*, *2011*, Article ID: 419. http://dx.doi.org/10.1109/ICSPS.2010.5555420.

[27] R. Yuvasri & A. Manimaran (2024). A secure key exchange protocol and a public key cryptosystem for healthcare systems. *Contemporary Mathematics*, *5*(2), 2491–2507. https://doi.org/10.37256/cm.5220243942.