AAECC (2016) 27:523–535
DOI 10.1007/s00200-016-0293-8

ORIGINAL PAPER

Undeniable signature scheme based over group ring

Neha Goel[1] · **Indivar Gupta**[2] · **M. K. Dubey**[2] · **B. K. Dass**[1]

Received: 20 November 2015 / Revised: 16 April 2016 / Accepted: 4 May 2016 /
Published online: 4 June 2016

Abstract D. Chaum and H. van Antwerpen first introduced the concept of an undeniable signature scheme where the verification step is verified with the signer's co-operation. In this paper, first we discuss a combination of Discrete Logarithm Problem (DLP) and Conjugacy Search Problem (CSP) analysing its security. Then we propose an undeniable signature scheme in a non-abelian group over group ring whose security relies on difficulty of the combination of the DLP and the CSP. The complexity and security of our proposed scheme has also been discussed.

Keywords Conjugacy Search Problem · Discrete Logarithm Problem · Group ring · Undeniable signatures

Mathematics Subject Classification 94A60

1 Introduction

Conventional signatures simply reveals the identity of a person who has signed a particular document or message, so that a receiver is able to know the origin of message. But conventional signatures are not preferable everywhere during communication as these can be easily copied and misused. Therefore to maintain authenticity and integrity of a message, "Message Authentication Code (MAC)" was proposed. In MACs, a message and a secret key are taken as an input to get an authentication code as an output. This authentication code is termed as *tag*, which is sent to a receiver along

✉ Neha Goel
nehagoel_7@yahoo.com

[1] University of Delhi, Delhi 110-007, India

[2] Scientific Analysis Group, DRDO, Metcalfe House, Delhi 110-054, India

with the message. The receiver uses a verification algorithm to verify whether the received *tag* is valid or not. MACs failed to satisfy the following properties [1]:

- the non-repudiation property,
- the publicly verifiable property.

Also if a signer wants to communicate with multiple receivers, he has to calculate and maintain a secret key as well as the *tag* corresponding to each receiver which is a quite tedious job. To overcome these limitations, Diffie–Hellman [2] introduced the notion of digital signature in 1976. At the same time an RSA based digital signature scheme was proposed in [3] and after that several digital signature schemes were proposed like ElGamal's Signature Scheme [4], Digital Signature Algorithm (DSA) [4] and so on. All these digital signature schemes have the universal verifiable property which is not desirable in certain cases.

In [5], Chaum and van Antwerpen introduced the concept of undeniable signatures whose security relies on the hardness of the DLP. In undeniable signatures, signer's co-operation is required at verification step and the signer cannot deny validity of a signature. Undeniable signatures also consists of a disavowal protocol which is used when a receiver gets an invalid signature. Using disavowal protocol, the receiver can easily find out the reason of an invalid signature, that is, whether the signature is invalid due to forgery or the signer's fault who has not cooperated properly in verification protocol. After Chaum and Antwerpen's scheme over the DLP, some more undeniable signature schemes were proposed whose security relies on the different computational hard problems like the Integer Factorization Problem (IFP) [6], the CSP [7], the Elliptic Curve Discrete Logarithm Problem (ECDLP) [8], etc.

In [9–11], some cryptographic protocols were proposed whose security simultaneously relies on the two computational hard problems, the DLP and the CSP. In [9], a key exchange protocol based on a combination of the DLP and the CSP was defined using polycyclic groups which was named as Power Conjugacy Search Problem. The combination of the DLP and the CSP was defined in [10] using group representation and a key exchange protocol was proposed over it. Further in [11], the same combination was used to define Diffie–Hellman key exchange protocol and ElGamal's cryptosystem in a non-abelian group over group ring.

Our contribution In this paper we discuss a combination of the DLP and the CSP which is termed as DLCSP and define it over a non-abelian group. Further we analyse its brute force complexity thoroughly using security parameters.

We noticed that complexity of this new problem DLCSP is much greater than that of the DLP and other existing computationally hard problems like the IFP and the CSP. It provides same security as other existing computationally hard problems but with less size of parameters. We consider that the DLCSP is a better computational hard problem for defining cryptographic protocols and; therefore, we propose an undeniable signature scheme whose security relies on hardness of the DLCSP in a non-abelian group over group ring. We also discuss the security and complexity of the proposed scheme.

The paper is organized in the following manner. In Sect. 2, we give preliminaries require for understanding of the paper. In Sect. 3, we discuss a combination of the

DLP and the CSP. In Sect. 4, an undeniable signature scheme based on non-abelian group over group ring is proposed and the classical security of the scheme is analysed. Finally, we conclude the conclusion.

2 Preliminaries

To proceed with our proposed undeniable signature scheme, we require the following definitions.

Definition 1 (*Group-Ring*) Let K be a field and G be a multiplicative group, finite or infinite. Then the group ring denoted by $K[G]$ is defined as an associative algebra consisting of all formal finite sums of the form

$$\alpha = \sum_{x \in G} a_x x$$

where $a_x \in K$. If $\beta = \sum_{x \in G} b_x x$ is another element of $K[G]$, then addition and multiplication are defined by:

$$\alpha + \beta = \left(\sum_{x \in G} a_x x \right) + \left(\sum_{x \in G} b_x x \right) = \sum_{x \in G} (a_x + b_x)\, x$$

and

$$\alpha\beta = \left(\sum_{x \in G} a_x x \right) \left(\sum_{y \in G} b_y y \right) = \sum_{x,y \in G} (a_x b_y xy) = \sum_{z \in G} c_z z$$

where,

$$c_z = \sum_{xy=z} a_x b_y = \sum_{x} a_x b_{x^{-1}z} = \sum_{y} a_{zy^{-1}} b_y.$$

Example 1 Let $K = \mathbb{F}_5$ be a finite field of order 5 and $G = S_3$ be a symmetric group on three symbols. Then the group ring is denoted by $\mathbb{F}_5[S_3]$.

For further details on group ring, reader may refer [12].

Definition 2 (*Conjugacy Search Problem*) The Conjugacy Search Problem in a non-abelian group $(G, \cdot)$ is defined as follows: for given $x, y \in G$ such that $x = a^{-1} \cdot y \cdot a$, find $a \in G$.

Definition 3 (*Discrete Logarithm Problem*) Given a prime p, a generator α of $\mathbb{Z}_p^*$ and an element $\beta \in \mathbb{Z}_p^*$ where $\mathbb{Z}_p^*$ is a cyclic group, find an integer x, $0 \leq x \leq p-2$ such that $\alpha^x \equiv \beta \pmod{p}$.

The choice of G and p in Definitions 2 and 3 respectively depends on the security level which designer wants to achieve in the cryptosystem. For further references on the CSP and the DLP reader may refer [13] and [4] respectively.

2.1 Undeniable signature scheme over DLP

The concept of undeniable signature was established by Chaum and van Antwerpen [5]. The main difference between undeniable signatures and digital signatures is, in undeniable signatures both verifier and signer cooperates at verification step, which is not the case of digital signatures. The undeniable signature scheme proposed in [5] is defined as follows.

2.1.1 The scheme

Set-Up: Let $p = 2q + 1$ be a prime, where q is also a prime. Let $\mathcal{G}$ be a subgroup of $\mathbb{Z}_p^*$ of order q.

Key-Gen: Let α be an element of order q in $\mathbb{Z}_p^*$ and $\beta \equiv \alpha^a \bmod p$, where $1 \leq a \leq q-1$. Then public key of the signer is $pk = (p, \alpha, \beta)$ and secret key is $sk = a$.

Sign-Gen: To sign a message $x \in \mathcal{G}$, the signer computes $y \equiv x^a \bmod p$ and sends (x, y) to the verifier as signature.

Verification Protocol: The verification protocol comprises of the following steps:

Step 1. The verifier picks random $e_1, e_2 \in \mathbb{Z}_q^*$ computes $c = y^{e_1}\beta^{e_2} \bmod p$ and $d = x^{e_1}\alpha^{e_2} \bmod p$. Then sends c to the signer and kept d for further verification.
Step 2. The signer computes $d' = c^{a^{-1} \bmod q} (\bmod p)$ and sends d' to the verifier.
Step 3. The verifier compares this received d' with d. If $d = d'$ then the signature is accepted otherwise not.

Disavowal Protocol: Suppose at verification step the verifier notices that the signature is not valid, then using disavowal protocol the verifier can judge the reason behind invalid signature that is, whether the signer is showing dishonesty at verification time or the signature is forged. The protocol is defined as follows:

Step 1. The verifier picks random $e_1, e_2 \in \mathbb{Z}_q^*$ and sends $c = y^{e_1}\beta^{e_2} \bmod p$ to the signer.
Step 2. The signer computes $d = c^{a^{-1} \bmod q} \pmod p$ and sends it to the verifier.
Step 3. The verifier computes $d' = x^{e_1}\alpha^{e_2} \bmod p$ and notice that $d \neq d'$.
Step 4. The verifier again picks random $f_1, f_2 \in \mathbb{Z}_q^*$, calculates $C = y^{f_1}\beta^{f_2} \bmod p$ and sends it to the signer.
Step 5. The signer computes $D = C^{a^{-1} \bmod q} (\bmod p)$ and sends it to the verifier.
Step 6. The verifier again computes $D' = x^{f_1}\alpha^{f_2}$ and notice that $D \neq D'$.
Step 7. The verifier conclude that the signature y is forged if and only if

$$(d\alpha^{-e_2})^{f_1} \equiv (D\alpha^{-f_2})^{e_1}.$$

3 Discrete Logarithm Problem with Conjugacy Search Problem (DLCSP)

The DLP and the CSP, are basic ingredients of many cryptographic protocols. The DLCSP is defined as follows:

Definition 4 *(DLCSP)* Let $(H, \cdot)$ be a finite non-abelian group of order η and $\mathbb{Z}_p^*$ be a finite cyclic group.[1] Let x, y, z be arbitrary elements of H and a be a random element[2] of $\mathbb{Z}_p^*$. Then for given $y, z \in H$ such that $y = xz^a x^{-1}$, find $x \in H$ and $a \in \mathbb{Z}_p^*$.

If one of the secret parameter x or a is given then the DLCSP problem will reduce either to the DLP or the CSP that is,

- if x is given, the equation $y = xz^a x^{-1}$ will reduce to $x^{-1}yx = y' = z^a$. The problem is now to find 'a' for given $y' = z^a$ which is the DLP,
- if a is given, the equation $y = xz^a x^{-1}$ will reduce to $y = xz'x^{-1}$ where, $z' = z^a$. The problem is now to find x for given conjugates y, z' which is the CSP. Some example of groups in which the CSP is assumed to be hard are: Thompson's group, Groups of matrices, Solvable groups etc.

Thus the DLCSP is the combination of the DLP and the CSP. The complexity of the DLCSP and level of security of cryptosystem based on the DLCSP will depend on size of H and p.

3.1 Brute force complexity of DLCSP

Let $H = \{x_1, x_2, \ldots, x_j, \ldots, x_\eta\}$ be a non-abelian group and $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$, then the DLCSP is to find $x \in H, i \in \mathbb{Z}_p^*$ for given $y, z \in H$ such that $y = xz^i x^{-1}$. Here x, y, z can be expressed as $x = x_j, y = x_k, z = x_l$, where $j, k, l \in \{1, 2, \ldots, \eta\}$. The steps for solving the DLCSP against exhaustive search method are discussed in algorithm 1.

Thus, total number of steps to solve the DLCSP are $O(\eta p)$ which is exponential in the size of ηp in bits that is $e^{\log_e 2 \cdot \log_2(\eta p)} = e^{c \cdot size(\eta p)}$ where, $c = log_e 2$.

Example 2 (*Complexity of the DLCSP in* $H = GL_n(\mathbb{F}_q[S_r])$)

Here, we discuss complexity of the DLCSP for a particular non-abelian group. Let $H = GL_n(\mathbb{F}_q[S_r])$ be a non-abelian group of $n \times n$ matrices of order η over group ring $\mathbb{F}_q[S_r]$, where $\mathbb{F}_q$ is a field and S_r is a symmetric group. Let X, Y, Z be three $n \times n$ matrices of H where X is non-degenerated matrix and $a \in \mathbb{Z}_p^*$ such that $Y = XZ^a X^{-1}$. Then number of operations required to find (X, a) are $O(\eta p)$ which is same as $O(\exp(\log_e \eta p))$.

[1] We can choose the set of positive integers of cardinality p (where p may or may not be prime) in place of finite cyclic group. $\mathbb{Z}_p^*$ is used only for exploring the DLCSP in an undeniable signature scheme.

[2] The choice of $a \in \mathbb{Z}_p^*$ and $z \in H$ should be such that $z^a \neq 1$.

Algorithm 1: Exhaustive Search Algorithm

Input: $y, z \in H$ such that $y = xz^i x^{-1}$
Output: Secret parameters $x \in H, i \in \mathbb{Z}_p^*$

```
for i ← 1 to p − 1 do
    z̄ ← z^i;
    for j ← 1 to η do
        y_j ← x_j z̄ x_j^{-1};
        Compare y = y_j;
        if y = y_j;
        return (x_j, i) & exit;
        else
            go to next step;
        j ← j + 1;
    i ← i + 1;
```

The advantage of taking $H = GL_n(\mathbb{F}_q[S_r])$ is that the matrix multiplication is very efficient in these groups [14] and these groups are improbable for applying attacks using eigenvalues and determinants [11]. Also the size of such groups increases rapidly even for small values of n, q and r.

3.2 Security parameters

In this section, we discuss the size of parameters (n, q, r and p) for a secure and an efficient application of the DLCSP over a non-abelian group $H = GL_n(\mathbb{F}_q[S_r])$ and a finite cyclic group $\mathbb{Z}_p^*$. In particular, for $r = 3$ and $n = 2$ order of H can be computed as follows:

Using Wedderburn [15, theorem 2.17], [15, theorem 3.2] and [11, lemma 4.1.1] we have,

$$\mathbb{F}_q[S_3] \simeq \mathbb{F}_q \oplus \mathbb{F}_q \oplus Mat_2(F_q) \quad \text{(where } \mathbb{F}_q \text{ is not of characteristic 2 or 3)} \tag{1}$$

$$GL_2(\mathbb{F}_q[S_3]) \simeq GL_2(\mathbb{F}_q) \oplus GL_2(\mathbb{F}_q) \oplus GL_4(\mathbb{F}_q). \tag{2}$$

Hence,

$$|GL_2(\mathbb{F}_q[S_3])| = [(q^2-1)(q^2-q)]^2[(q^4-1)\cdots(q^4-q^{4-1})] > q^{16}. \tag{3}$$

Therefore, to achieve the security of order 2^{128} we may choose a prime q of size approximately 2^5 [this parameter gives $|H| \simeq 2^{80}$ from (3)]. Also, the size of the prime p should be taken greater than or equal to 48 bits.

4 Undeniable signature scheme based on group ring

In this section, we propose a new undeniable signature scheme whose security relies on the DLCSP which is defined in Sect. 3. The signature scheme is elucidated as follows.

Set-Up: Let $H = GL_n(\mathbb{F}_q[S_r])$ be a non-abelian group (as discussed in Example 1) and N be an abelian subgroup of H. Let $\hbar$ be a hash function defined as $\hbar : (0,1)^* \mapsto H\backslash N$.

Key-Gen: Let A be an element of $H\backslash N$ and $P = XA^aX^{-1}$ where $X \in N$ and $a \in \mathbb{Z}_p^*\backslash\{1\}$. Then, signer's public key is $pk = P$ and the private key is $sk = (X, a)$ and A is the public parameter.

Sign-Gen: A signature on a message $m \in (0,1)^*$ is $S = Y(\hbar(m))^aY^{-1} = XA^a(\hbar(m))^aA^{-a}X^{-1}$, where $\hbar(m) \in H\backslash N$ and $Y = XA^a$.

Verification Protocol: A verifier carries out the following steps to verify validity of the signature S:

Step 1. On receiving the signature S on the message m, the verifier picks a random matrix $R \in N$, a random integer $b \in \mathbb{Z}_p^*\backslash\{1\}$ and then computes $C = (RP^{-1}SPR^{-1})^b$ and sends C to the signer.
Step 2. The signer computes $Q = (X^{-1}CX)^{a^{-1}}$ and sends Q to the verifier.
Step 3. The verifier now calculates $Q_1 = R(\hbar(m))^bR^{-1}$ and checks whether $Q = Q_1$ or not.
Step 4. The signature is valid if and only if $Q = Q_1$.

We now discuss the completeness and soundness of the verification protocol:

Completeness and Soundness of the Verification Protocol: The completeness and soundness of the verification protocol can be verified from the following theorems.

Completeness: The verification protocol is said to be complete, if the verifier always accepts the signature when the signer and the verifier performed the verification protocol in specified manner.

Theorem 1 *The verification protocol is complete if the equality $Q = Q_1$ always holds.*

Proof On receiving the signature S on m, the verifier calculates $C = (RP^{-1}SP\ R^{-1})^b$ and sends it to the signer, then the signer calculates $Q = (X^{-1}CX)^{a^{-1}}$ using private key (X, a) and sends it to the verifier. The verifier then checks whether $Q = Q_1$ or not. The equality $Q = Q_1$ can be verified as follows:

$$
\begin{aligned}
Q &= (X^{-1}CX)^{a^{-1}} = X^{-1}C^{a^{-1}}X \\
&= X^{-1}\{(RP^{-1}SPR^{-1})^{b}\}^{a^{-1}}X \\
&= X^{-1}\{(R(XA^{-a}X^{-1})(XA^{a}\hbar(m)^{a}A^{-a}X^{-1})(XA^{a}X^{-1})R^{-1})^{b}\}^{a^{-1}}X \\
&= X^{-1}\{(R(X\hbar(m)^{a}X^{-1})R^{-1})^{b}\}^{a^{-1}}X \\
&= X^{-1}(RX\hbar(m)^{aba^{-1}}X^{-1}R^{-1})X \\
&= X^{-1}(XR\hbar(m)^{aa^{-1}b}R^{-1}X^{-1})X \\
&= R(\hbar(m))^{b}R^{-1} \\
&= Q_1.
\end{aligned}
$$

Thus, on receiving Q, the verifier verifies the equality $Q = Q_1$ and if the equality holds the verifier accepts the signature. □

Soundness: The verification protocol is said to be sound if a dishonest signer will not be able to convince the verifier for accepting an invalid signature.

Theorem 2 *The probability that the dishonest signer will be able to convince the verifier for accepting an invalid signature is not greater than maximum of* $\left(\frac{1}{\overline{\eta}p}, \frac{1}{\eta-\overline{\eta}}\right)$ *where,* $\overline{\eta}$ *is the order of* N *and* η *is the order of* H.

Proof On receiving $C = (RP^{-1}SPR^{-1})^{b}$ from the verifier, the dishonest signer will either try to extract the pair (R, b) to compute Q such that $Q = Q_1$ or the dishonest signer will simply select an element $\overline{Q} \in H \backslash N$ such that $\overline{Q} = Q_1$.

In first case, the probability of choosing correct pair (R, b) is not greater than $\frac{1}{\overline{\eta}p}$ where $R \in N$ and $b \in \mathbb{Z}_p^* \backslash \{1\}$. In second case, the probability is not greater than $\dfrac{1}{\eta - \overline{\eta}}$. □

4.1 Disavowal protocol

The role of disavowal protocol comes into picture when the verifier gets an invalid signature. The signature may be invalid in following two situations:

- The signer shows dishonesty at verification step,
- message is forged in an unauthorized manner.

Using disavowal protocol the verifier can judge which of above situation has occurred.

In the verification protocol, if the verifier finds that $Q \neq Q_1$ that is, $Q \neq R(\hbar(m))^{b}R^{-1}$ then the verifier follows one more round with new random elements $R_1 \in N$ and $b_1 \in \mathbb{Z}_p^* \backslash \{1\}$. After this the verifier computes $C_1 = (R_1 P^{-1} SPR_1^{-1})^{b_1}$ and sends it to the signer. Then on receiving $Q_2 = (X^{-1}C_1X)^{a^{-1}}$ from the signer, the verifier again notices that $Q_2 \neq R_1(\hbar(m))^{b_1}R_1^{-1}$ and concludes that $\hbar(m)$ is forged if and only if

$$RQ_2^{b}R^{-1} = R_1 Q^{b_1} R_1^{-1}. \tag{4}$$

Completeness and Soundness of Disavowal Protocol: Completeness and soundness of the disavowal protocol can be verified from the following theorems.

Completeness: The disavowal protocol is said to be complete if the verifier is always able to conclude that the signature over the message m is forged.

Theorem 3 *The disavowal protocol is complete if for* $S \neq XA^a(\hbar(m))^a A^{-a}X^{-1}$, *the verifier always get*

$$RQ_2^bR^{-1} = R_1Q^{b_1}R_1^{-1}.$$

Proof First we calculate left hand side of equality,

$$\begin{aligned}
RQ_2^bR^{-1} &= R(X^{-1}C_1X)^{ba^{-1}}R^{-1} \\
&= R(X^{-1}(R_1(XA^{-a}X^{-1})(XA^a(\hbar(m))^aA^{-a}X^{-1})(XA^aX^{-1})R_1^{-1})^{b_1}X)^{ba^{-1}}R^{-1} \\
&= R(X^{-1}(R_1(X(\hbar(m))^aX^{-1})R_1^{-1})^{b_1}X)^{ba^{-1}}R^{-1} \\
&= R(X^{-1}(X(R_1(\hbar(m))^{ab_1}R_1^{-1})X^{-1})X)^{ba^{-1}}R^{-1} \\
&= R(R_1(\hbar(m))^{ab_1}R_1^{-1})^{ba^{-1}}R^{-1} = R(R_1(\hbar(m))^{aa^{-1}b_1}R_1^{-1})^bR^{-1} \\
&= RR_1(\hbar(m))^{bb_1}R_1^{-1}R^{-1}. \qquad (5)
\end{aligned}$$

In similar manner calculation of right hand side equality gives,

$$R_1Q^{b_1}R_1^{-1} = R_1R(\hbar(m))^{bb_1}R^{-1}R_1^{-1}. \qquad (6)$$

Now, equating (5) and (6) we get

$$RQ_2^bR^{-1} = R_1Q^{b_1}R_1^{-1}.$$

□

Soundness: The disavowal protocol is said to be sound if the dishonest signer will not be able to convince the verifier for accepting a valid signature as a fraud signature.

Theorem 4 *The probability that the dishonest signer will succeed to convince the verifier for accepting a valid signature as a fraud signature, is not greater than maximum of* $\left(\frac{1}{\overline{\eta}p}, \frac{1}{\eta-\overline{\eta}}\right)$ *where,* $\overline{\eta}$ *is the order of* N *and* η *is the order of* H.

Proof Let us assume that $S = XA^a(\hbar(m))^aA^{-a}X^{-1}$ is a valid signature on $\hbar(m)$. The dishonest signer will be able to convince the verifier that S is a forged signature if the following assumption holds,

$$Q \neq R(\hbar(m))^bR^{-1}, \quad Q_2 \neq R_1(\hbar(m))^{b_1}R_1^{-1} \text{ and } RQ_2^bR^{-1} = R_1Q^{b_1}R_1^{-1}. \qquad (7)$$

But with this assumption we will arrive at a contradiction as discussed below.

From Eq. (4), we have,

$$Q_2 = R^{-1}(R_1 Q_{A_1}^{b_1} R_1^{-1})^{b^{-1}} R$$
$$= R_1(R^{-1}Q^{b^{-1}}R)^{b_1} R_1^{-1} = R_1 \mathcal{H}^{b_1} R_1^{-1} \text{ where, } \mathcal{H} = R^{-1}Q^{b^{-1}}R.$$

From soundness property of the verification protocol, probability that S is an originally valid signature for $\mathcal{H}$ is minimum of $\left(1 - \frac{1}{\overline{\eta}p}, 1 - \frac{1}{\eta - \overline{\eta}}\right)$ but S is a valid signature for $\hbar(m)$. This implies that, $XA^a(\hbar(m))^a A^{-a} X^{-1} = XA^a \mathcal{H}^a A^{-a} X^{-1}$ that is $\hbar(m) = \mathcal{H}$ with the probability minimum of $\left(1 - \frac{1}{\overline{\eta}p}, 1 - \frac{1}{\eta - \overline{\eta}}\right)$.

Again from Eq. (7),

$$Q \neq (R(\hbar(m))^b R^{-1})$$

that is,

$$\hbar(m) \neq R^{-1}Q^{b^{-1}}R = \mathcal{H}$$

which is a contradiction. Therefore, our assumption that $S = XA^a(\hbar(m))^a A^{-a} X^{-1}$ is a valid signature on $\hbar(m)$ and Eq. (7) holds is wrong and the probability that $Q \neq R(\hbar(m))^b R^{-1}$, $Q_2 \neq R_1(\hbar(m))^{b_1} R_1^{-1}$ and $RQ_2^b R^{-1} = R_1 Q^{b_1} R_1^{-1}$ is not greater than maximum of $\left(1 - \left(1 - \frac{1}{\overline{\eta}p}\right), 1 - \left(1 - \frac{1}{\eta - \overline{\eta}}\right)\right)$ that is maximum of $\left(\frac{1}{\overline{\eta}p}, \frac{1}{\eta - \overline{\eta}}\right)$. □

Remark 1 It is important to note that the scheme is not considered to be a zero knowledge undeniable signature scheme. However, the scheme is secure and no secret parameter is revealed at the time of verification and in disavowal protocol.

4.2 Complexity and security analysis of the proposed undeniable signature scheme

Complexity and security analysis of the proposed undeniable signature scheme is given below.

4.2.1 Security analysis

The classical security of the undeniable signature scheme is discussed here.

Data Forgery: In this case, an adversary will try to replace the original message m with the forged message m'. For this, either the adversary will try to extract the private keys of the signer or try to find a message $m' \neq m$ such that $\hbar(m') = \hbar(m)$.

For the first case, the adversary will face the problem of solving the DLCSP which is computationally infeasible for selected parameters as discussed in Sect. 3.1.

The second case will also be computationally infeasible if the hash function used in designing of the scheme is pre-image resistant.

Existential Forgery: In this case, an adversary will try to create a valid signature for at least one message [4]. This can be done in following three ways:

Existential forgery by known message attack: Let $\mathcal{S}$ be a set of all signatures corresponding to the messages. Suppose an adversary selects a pair $(m, S) \in \mathcal{S}$ to forge the signature. For this the adversary will try to find a $m' \neq m$ such that $\hbar(m') = \hbar(m)$. But the use of second pre-image resistant function makes the scheme secure against this case. Even after this, if the adversary gets a $m \neq m'$ such that $\hbar(m) = \hbar(m')$ so that (m', S) is a valid signature then, at verification step adversary has to calculate Q using the secret parameters (X, a). But it is not feasible due to hardness of the DLCSP.

Existential forgery by chosen message attack: Suppose an adversary possess a set $\mathcal{S}$ of message signature pairs. The adversary will try to find two messages (m', m) such that $m' \neq m$ but their hash value is not same that is $\hbar(m') = \hbar(m)$ and (m', S) is a valid signature. The use of collision resistant hash function makes the scheme secure from this attack.

Again, let the adversary gets a message $m \neq m'$ such that $\hbar(m) = \hbar(m')$ and (m', S) is a valid signature. Then at the verification step, the adversary will face the problem to solve the DLCSP for computation of Q. Since the DLCSP is computationally hard problem as discussed in Sect. 3; therefore, the scheme is secure against existential forgery by chosen message attack.

Existential forgery by total break: In this case, an adversary will try to forge the signature without the knowledge of the message signature pairs. For this, the adversary will try to create a valid signature on some message. But the use of pre-image resistant hash function makes the scheme secure against this attack.

The probability of accepting an invalid signature by the verifier is discussed in Theorem 2.

Thus, the scheme is secure against existential forgery and the above discussion can be concluded as following theorem.

Theorem 5 *If an existential forgery exists then the DLCSP can be solved.*

Theorem 6 *The probability that the verifier accepts a fraud signature is at most* $\frac{1}{|H \backslash N|}$, *where* $|H \backslash N|$ *is the cardinality of* $H \backslash N$.

Proof Suppose an adversary tries to forge the signature. For this purpose the adversary will proceed the following steps:

- The adversary will pick $X' \in N$ and $a' \in \mathbb{Z}_p^* \backslash \{1\}$ then calculate $S' = X' A^{a'} \overline{\hbar(m)}^{a'} A^{-a'} X'^{-1}$ and sends $(\overline{\hbar(m)}, S')$ to the verifier.
- On receiving $(\overline{\hbar(m)}, S')$ and considering that the signature is genuine, the verifier calculates $C' = R P^{-1} S'^{b} P R^{-1}$ and sends C' to the signer.
- The adversary again intercepts in between and calculate $Q' = (X'^{-1} C' X')^{a'^{-1}}$. The adversary then sends it to the verifier.
- To verify the signature, the verifier calculates $Q'_1 = R \overline{\hbar(m)}^{b} R^{-1}$ and check whether $Q' = Q'_1$ or not.

If this equality holds then, the adversary will be succeeded in forging the signature. So to make this equality hold the adversary will pick the parameters in first step in such a manner that $Q' = Q'_1$ where, $Q', Q'_1 \in H\backslash N$.

Let η and $\overline{\eta}$ be the cardinality of H and N respectively, then the probability that $Q' = Q'_1$ is computed as follows:

Number of ways in which Q', Q'_1 can be taken from $H\backslash N$ as (Q', Q') or (Q'_1, Q'_1) that is $Q' = Q'_1$ are $\eta - \overline{\eta}$. Therefore, favourable number of cases are $\eta - \overline{\eta}$. Total number of ways of choosing (Q', Q'_1) from $H\backslash N \times H\backslash N$ are $(\eta - \overline{\eta})^2$. Hence, the probability that the verifier accepts a fraud signature is,

$$\frac{\eta - \overline{\eta}}{(\eta - \overline{\eta})^2} < \frac{1}{(\eta - \overline{\eta})} = \frac{1}{|H\backslash N|}.$$

The size of the abelian subgroup N should be taken in such a way that the variability of $H\backslash N$ remains sufficient. □

4.2.2 Complexity analysis

Total number of operations required in proposed undeniable signature scheme for key generation, signature generation, verification and disavowal protocol using the parameters described in Sect. 3 are discussed below.

Number of operations required in Key-Gen: For key-generation we need to calculate $P = XA^aX^{-1}$, where $A \in H\backslash N, a \in \mathbb{Z}_p^*\backslash\{1\}$. The matrices X, A are taken over group-ring $\mathbb{F}_q[S_r]$ and are of order n. The number of bit operations required to multiply two matrices of order n are at most $O(n^3)$ [16]. Therefore to calculate A^a, total number of operations will be $n^3 \log p$ [16]. Finally to calculate XA^aX^{-1}, we need $2n^3$ more operations. Thus the total number of operations required for Key-Gen are at most $n^3(\log p + 2)$ which is proportional to $O(n^3 \log p)$.

Number of operations required in Signature Generation: To generate a signature on a message m, we calculate $S = XA^a(\hbar(m))^aA^{-a}X^{-1}$. Therefore, the total number of bit operations required in signature generation are proportional to $O(n^3 \log p)$ as discussed in Key-Gen step.

Number of operations required in Verification Protocol: We apply the same procedure as above for calculating the number of operations in verification protocol. The total number of bit operations required to calculate $C(= (RP^{-1}SPR^{-1})^b)$ are $4n^3 \log p$. Then calculation of each term $Q\ (= (X^{-1}CX)^{a^{-1}})$ and $Q_1(= (R(\hbar(m))^bR^{-1}))$ will take $n^3 \log p$ operations. The comparison in step 4, of verification protocol takes 1 operation. Therefore, the total number of bit operations required in verification of signature are $5n^3 \log p + 1$ which is proportional to $O(n^3 \log p)$.

Number of operations required in Disavowal Protocol: The disavowal protocol contains one more round than verification protocol; therefore, the total number of operations in disavowal protocol are $10n^3 \log p + 2$ which is proportional to $O(n^3 \log p)$.

5 Conclusion

In this paper, we have discussed a combination of the DLP and the CSP in a non-abelian group and termed this combination as DLCSP. We analysed the complexity of the DLCSP with respect to security parameters. We then proposed an undeniable signature scheme in a non-abelian group over group ring whose security relies on the DLCSP. Finally, we analysed the classical security and time complexity of the proposed scheme.

Acknowledgments The authors would like to express their sincere thanks to the reviewers of the manuscript for their valuable comments and suggestions which were very useful to improve the manuscript. The authors are grateful to the editorial board of the journal for their support and co-operation. The authors are also thankful to the Director SAG for allowing us to pursue this work.

References

1. Katz, J., Lindell, Y.: Introduction to Modern Cryptography. Chapmen & Hall/CRC Press, Taylor & Francis, London (2007)
2. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. Inf. Theory **22**, 644–654 (1976)
3. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signature and public-key cryptosystem. Commun. ACM **21**, 120–126 (1978)
4. Stinson, D.R.: Cryptography Theory and Practice, Second Indian Reprint. Chapman & Hall/CRC Press, London (2013)
5. Chaum, D., van Antwerpen, H.: Undeniable signatures. In: Advances in Cryptology-CRYPTO'89. Lecture Notes in Computer Science, vol. 435, pp. 212–216 (1990)
6. Gennaro, R., Krawczyk, H., Rabin, T.: RSA-based undeniable signatures. J. Cryptol. **13**, 397–416 (2000)
7. Thomas, T., Lal, A.K.: A zero-knowledge undeniable signature scheme in non-abelian group setting. Int. J. Netw. Secur. **6**, 265–269 (2008)
8. Chen, T.-S., Hsu, E.-T., Yu, Y.-L.: A new elliptic curve undeniable signature scheme. Int. Math. Forum **1**(31), 1529–1536 (2006)
9. Kahrobaei, D., Khan, B.: A non-commutative generalisation of ElGamal key exchange using polycyclic groups. In: Global Telecommunication Conference, GLOBECOM, IEEE, pp. 1–5 (2006)
10. Sakalauskas, E., Tvarijonas, P., Raulynaitis, A.: Key agreement protocol using conjugacy search problem and discrete logarithm problem in group representation level. Informatica **18**, 115–124 (2007)
11. Eftekhari, M.: A Diffie–Hellman key exchange protocol using matrices over non-commutative rings. Groups Complex. Cryptol. **4**, 167–176 (2012)
12. Passman, D.S.: The Algebraic Structure of Group Ring. Wiley, New York (1977)
13. Myasnikov, A., Shpilrain, V., Ushakov, A.: Non-commutative Cryptography and Complexity of Group-Theoretic Problems, vol. 177. American Mathematical Society, Providence (2011)
14. Kahrobaei, D., Koupparis, C., Shpilrain, V.: Public key exchange using matrices over group ring. Cryptology eprint Archive Report 2013/114. https://eprint.iacr.org/2013/114
15. Dornhoff, L.: Group Representation Theory (Part A). Marcel Dekker, New York (1971)
16. Koblitz, N.: A Course in Number Theory and Cryptography, 2nd edn. Springer, New York (1994)