J. Integr. Sci. Technol. 2023, 11(2), 471

Integrated Science

Journal of Integrated
SCIENCE& TECHNOLOGY

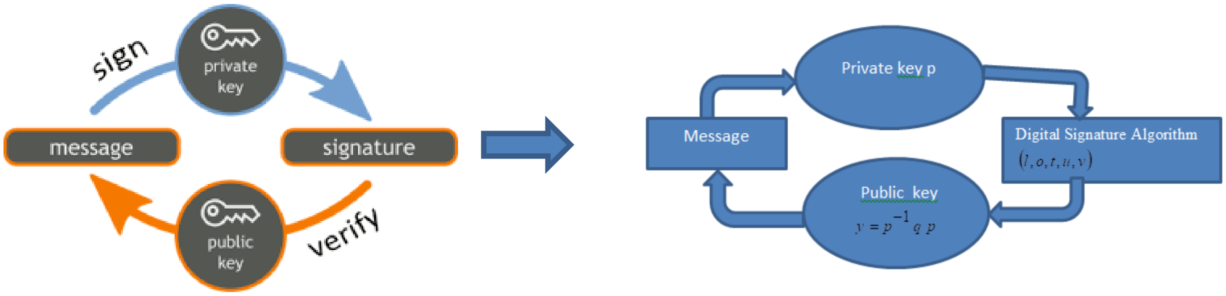
New Digital Signature Scheme on Non-Commutative Rings using Double Conjugacy

V. Jalaja,[1] G.S.G.N. Anjaneyulu,[2] L. Narendra Mohan[2*]

[1]*Department of Mathematics, Sree Vidyanikethan Engineering College, Tirupati, Andhra Pradesh 517102. India.* [2]*Department of Mathematics, SAS, Vellore Institute of Technology, Vellore, Tamil Nadu 632014. India.*

Received on: 18-Oct-2022, Accepted and Published on: 21-Nov-2022

ABSTRACT



Digital signature algorithm provides a security of a message which is transferred from one person to another person. Many algorithms have been designed by taking single hard problems like Discrete logarithm problem, Integer factorization problem, Conjugacy problem, however, it has been observed that above algorithms are hard to compute towards finding a proper solution. Nowadays most of the algorithms are designed by combination of two hard problems. We designed an algorithm to provide equivalent security with one hard problem. In this article we designed a new digital signature scheme based on the Conjugacy problem in non-commutative rings. Initially we presented a signature scheme by using double Conjugacy over non-commutative rings. The strength of the algorithm was demonstrated using the confirmation theorem and further security analysis has been performed.

Keywords: Digital Signature, Conjugacy Problem, Double Conjugacy Problem, Non-Commutative Ring.

INTRODUCTION

A digital signature is an authentication mechanism that allows the author of the communication to assign a code to the message that serves as a signature. It fulfils the objectives of authenticity, integrity, and non-repudiation by acting as a handwritten signature. Handwritten signatures are commonly used to authenticate paper documents. Similarly, electronic documents can be verified using a signature known as a digital signature.In digital signatures, a general concept is designed to create a good working region, find hard problems in this structure, create a one-way function referencing these hard problems, and then build an algorithm. It is used to solve the intractable problems directly related to number theory rather than group theory.

The concept of Public Key Cryptography (PKC) was first used by Diffie & Hellman (DH) in 1976.[1] The main idea for PKC is to remove difficulty of key sharing in symmetric-key cryptography, in which different key is desirable for both the users to communicate in confidential. If there are n users who want to exchange secret data using symmetric-key cryptography, there are nc_2 keys needed and this number increases rapidly as the number of users grows. In PKC, each user generates a couple of keys, one is public/open and other is to be kept secret. Open key is referred as “public-key” used for encryption and secret-key is referred as “private-key” for decryption. Here no key is shared like symmetric key cryptography. In this area new notable reach of PKC is constructing digital signature scheme, which is a part of PKC. Here private-key is used for signature generation and public-key is used for signature verification. Hash functions are used for data integrity in conjunction with digital signature schemes[6], where for several

*Corresponding Author L.Narendra Mohan, VIT, Vellore
Tel:9885194025
Email: mohan.narendra3@gmail.com

Cite as: *J. Integr. Sci. Technol., 2023, 11(2), 471.*
URN: NBN:sciencein.jist.2023.v11.471

ISSN: 2321-4635
http://pubs.thesciencein.org/jist

causes; a message is typically hashed first, and then hash value becomes representative of message, signed in place of original message. Different class's hash functions are named as message authentication codes (MAC) allows message authentication by symmetric techniques.[2] J. Mo, et.al., explained a scheme by using key agreement protocol. In this scheme both the members have to design their own private key for sending a message. At the end of the algorithm, both the persons have to verify for the authentication of a message.[3]

Now a days most of the algorithms are based on the combination of prime factorization and discrete logarithms problems, but each one has its own set of defects and attacks. The difficulty of solving a set of challenging theoretical issuesmodern cryptography is used . As long as the problem on which they are based is secure, these algorithms are secure.[4-5]

Ismail E.S.et.al., proposed a signature scheme using factor problem and discrete logarithm problem.[6] They used both the hard problems in signing and verification equations. Also they showed that the scheme is secure against the most five attacks and also discussed the time complexity of an algorithm. P.V.Reddyet.al., presented a scheme by selecting the polynomials randomly in the given non-commutative algebraic system.[7] The proposed scheme is more secure, since this algorithm is developed under the non-commutative structure. This is the first digital signature schemes based on polynomial symmetrical decomposition on non-commutative algebraic systems. A.Raulynaitis et. al., presented an article, in that they used Conjugator search problem and modified discrete logarithm problem. The modified discrete logarithm problem is used in word equivalence problem for proving security.[8]

Sushila et.al., presented an algorithm, with the help of two hard mathematical problems like factorization and discrete logarithm problem, since most of the algorithms involves only one hard problem like prime factorization problem, elliptic curve problem, discrete logarithm problem.[9] Sushila et.al. explained the different weaknesses and attacks of the previously developed algorithms. They also explained the concept that if one can find a solution of both the problems simultaneously for attacking this algorithm. It is not possible, because the algorithm is designed by taking multiple hard problems.[9]

S.Kim presented a method for solving the Conjugacy problem for finitely generated free groups.[10] They mentioned that the Conjugacy problem[23] is solved if the length of the elements $z \in G$ must satisfy. This approach is simple to use for a computer search for $\phi \in$ End(G) having residual. Wei Bi et.al.,[7]expressed a secure digital signature algorithm for block chain by using elliptic curves. Some authors are used backdoor system in ECDSA to avoid, they introduced this algorithm.[11] This system is flexible to choose the number of elliptic curves and need to specify the parameters of each elliptical curve.

Khatoone et.al., developed a scheme by providing high level security with the help of NKAP-ECDH-SET. Also they provided the authentication of the message, they also showed that the computation cost is low.[12]

A.G. Reddy et.al., developed a privacy preserving three factor authenticated key agreement protocol for client-server environment. They established a scheme by using unique key agreement protocol. By using unique key they showed the execution time for algorithm is low when compared to other algorithms.[13]

Busom N et.al., Jalaja et.al., presented a scheme using homomorphic encryption with double Conjugacy problem in smart meter system. In this algorithm the double Conjugacy problem is used in both generation and verification process. So, it is more secure.[14-15]

Balasubramanian et.al., developed an algorithm based on elliptic curves to provide data integrity in the cloud.[16] They proposed above algorithm in cloud database and it is developed by using elliptic curves. S. Xiao et.al. discussed an algorithm based on Elliptic Curve Cryptography and it's applications in BITCOIN and Internet of Things.[17,31]

P. Liu et.al., presented a secured password dependent key agreement scheme. In this article they used password key agreement procedure in elliptic curve cryptography. The algorithm consists of 4 stages namely starting phase, registration phase, key authentication phase and accepting key phase.[18]

Narendra Mohan et. al., presented a scheme of Key agreement protocol and Cryptosystem on elliptic curves by using SET Protocol and compare the results to existing algorithms.[19]

Iswarya et al. proposed a non-abelian cryptosystem based on group elements.[20] In their work, they proposed a cryptosystem by non-commutative group elements with special word constructing through multiplication modulo property. Here they take normal group elements with positive integers. By using this cryptosystem, signature construction is also possible.

Elgamal Proposed digital signature scheme, the security is based on hardness of computing discrete logarithms in Z_p^*, where p is a prime number.[21] The key was generated by using Elgamal encryption system.

In many real life applications the researchers are using digital signature algorithm to provide security. This leads to the development of a Cryptographic application known as Digital Signature by solving difficult problems such as Conjugacy and Double Conjugacy, as well as increasing security.[22] Our proposal's main idea is that we treated the Conjugacy problem as NP-hard for a given set. In non-commutative algebraic structure, the Conjugacy problem is an unsolvable problem.

CRYPTOGRAPHIC ASSUMPTIONS IN CONJUGACY OVER NON-COMMUTATIVE RING

Define a Conjugacy problem, let us consider the non-commutative group G, and select two elements $p, q \in G$ are said to be conjugate to each other if $y = p^{-1} q\, p$ for some $p \in G$. The Conjugacy problem satisfies reflexive, symmetric and transitive. So, it is an equivalence relation.[23]

Double Conjugacy: Use of Conjugacy structure in Conjugacy problem is known as Double Conjugacy.

NEW PRESENTED DIGITAL SIGNATURE SCHEME USING DOUBLE CONJUGACY OVER NON-COMMUTATIVE RINGS

In this section, we are explaining how the proposed algorithm works and also by considering a set consists of matrices and we implementing the proposed scheme on that set. Mainly the algorithm consists of 3 stages namely Key generation, Signature generation and Signature verification. In the key generation phase, the public key's and private keys will generate.[24-25] The signature is generated and it can be act as a code for providing security of the message in the signature generation phase, finally the message is obtained by verifying the signature in the signature verification stage.

The following are the steps which describe the algorithm.

Initial setup

Consider $(S, +, .)$ be a non-commutative ring and we taken as the underlying work structure. Let the cryptographic hash function H is defined from S to the message space M $(i.e., \; H : S \to M)$

Key Generation

Assume a person A wants to send a document and a message M . She then sends it to the individual for verification. She first chooses p & q two random elements which are belongs to the set S and she computes $y = p^{-1} q\, p$ and publishes her public key's are y & q and p is her private key.[26]

Signature Generation

The person A performs the following.

A selects random element $r \in S$, the she defines

$l = r^{-1} q\, r$

$n = p^{-1} H(M)\, l\, p$

$o = r^{-1} n\, r$

$t = r^{-1} n\, p$

$u = p^{-1} H(M)\; r$

$v = r^{-1} H(M)\, r$

The message $(l, \; o, \; t, \; u, \; v)$ is then signed, and it is sent to B for verification and then for authentication.

Signature Verification

In signature verification, the person B receives the person A signature $(l, \; o, \; t, \; u, \; v)$, then the person B will do the following. He computes for this

$w = t\, y^{-1} u$

B accepts A 's signature if and only if

$l^{-1} v = o^{-1}\, w$

Otherwise, the signature is rejected.

The below is the flow chart which summarizes the above algorithm.

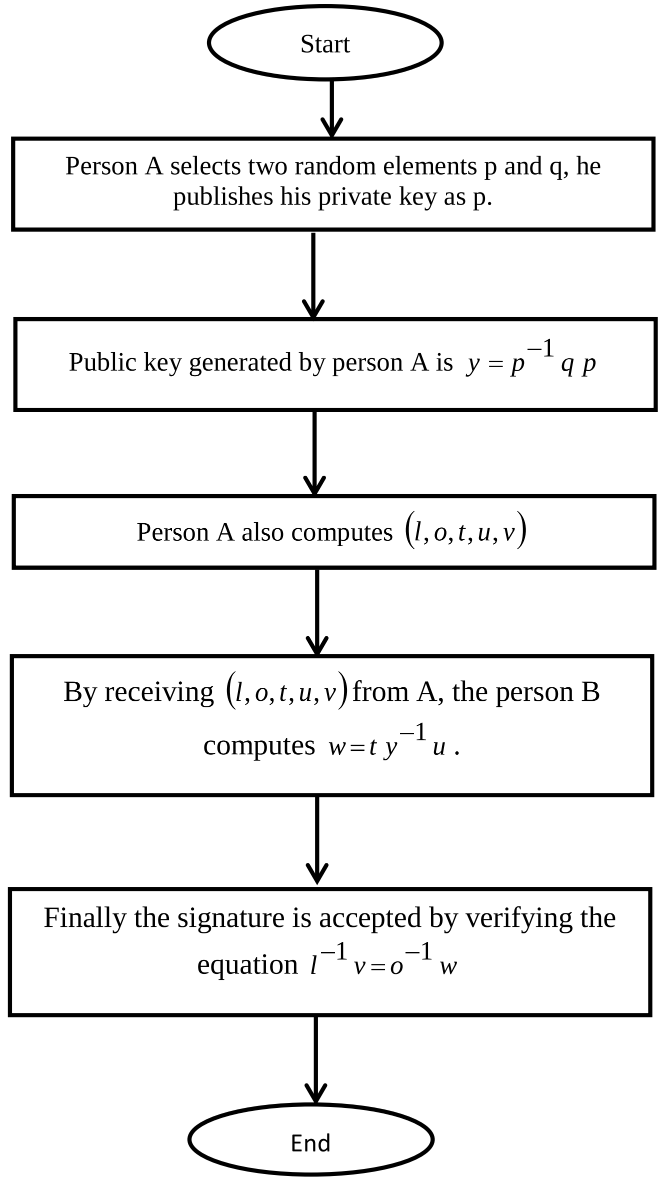

Start
Person A selects two random elements p and q, he publishes his private key as p.
Public key generated by person A is $y = p^{-1} q\, p$
Person A also computes (l, o, t, u, v)
By receiving (l, o, t, u, v) from A, the person B computes $w = t\, y^{-1} u$.
Finally the signature is accepted by verifying the equation $l^{-1} v = o^{-1} w$
End

Figure 1. Flowchart for the proposed algorithm

CONFIRMATION THEOREM

We are providing the strength of the proposed algorithm by proving the confirmation theorem in this section. This theorem states that "If the signature verification algorithm is followed, then the signature is always accepted as valid".

Proof:

For algorithm verification, both the persons have to calculate the following values.

$$l^{-1} v = \left(r^{-1} q r\right)^{-1} \left(r^{-1} H(M)\, r\right)$$

$$= r^{-1} q^{-1}\, r\, r^{-1}\, H(M)\, r$$

$$o^{-1}w = \left(r^{-1}n\,r\right)^{-1} t\,y^{-1}u$$

$$= \left(r^{-1}n^{-1}\ r\right)\left(r^{-1}n\ p\right)\left(p^{-1}q\,p\right)^{-1}\left(p^{-1}H(M)\,r\right)$$

$$= r^{-1}n^{-1}\ r\,r^{-1}n\ p\,p^{-1}\ q^{-1}\ p\,p^{-1}H(M)\,r$$

$$= r^{-1}q^{-1}H(M)\,r$$

$$\therefore\ l^{-1}v = o^{-1}w$$

EXAMPLE

We use a non-commutative matrix ring to validate the above digital signature scheme.

Initial setup

Assume, we choose S is $2X2$ matrix ring with the normal addition and multiplication operations.[27-29]
Define

$$M_2\left(Z_P\right)=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in Z_p,\ \mathit{for\ prime\ p\ and}\ \ ad-bc \neq 0\right\}$$ and

$S = M_2\left(Z_p\right) \cup \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$; where p is secure prime. Then $(S,\ +,\ .)$ is clearly non-commutative ring.

Let cryptographic hash function H is a mapping from S to the message space M $(i.e., H : S \to M)$ and it is defined by $m_{ij} \to 2^{m_{ij}}$ mod p for $m_{ij} \in M_2\left(Z_p\right)$. We choose $p = 13$ and all calculations in the multiplication modulo 13 group were chosen and evaluated.

Key Generation

In key generation phase, the person A choose $x = \begin{bmatrix} 2 & 3 \\ 5 & 4 \end{bmatrix} \in S$ and a random polynomial $6x^2 + 8x + 9$ such that $p = 6x^2 + 8x + 9$.

So, $p = 6\begin{bmatrix} 2 & 3 \\ 5 & 4 \end{bmatrix}^2 + 8\begin{bmatrix} 2 & 3 \\ 5 & 4 \end{bmatrix} + 9\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 13$

$= \begin{bmatrix} 139 & 132 \\ 220 & 227 \end{bmatrix} \bmod 13$

$= \begin{bmatrix} 9 & 2 \\ 12 & 6 \end{bmatrix}$ as her private key and then computes public key by randomly choosing q as $3x^2 + 6x + 1$.

So, $q = 3\begin{bmatrix} 2 & 3 \\ 5 & 4 \end{bmatrix}^2 + 6\begin{bmatrix} 2 & 3 \\ 5 & 4 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$= \begin{bmatrix} 70 & 72 \\ 120 & 118 \end{bmatrix} \bmod 13$

$= \begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}$

$\therefore y = p^{-1}q\,p = \begin{bmatrix} 9 & 2 \\ 12 & 6 \end{bmatrix}^{-1}\begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 9 & 2 \\ 12 & 6 \end{bmatrix}$

$= \begin{bmatrix} 8 & 6 \\ 10 & 12 \end{bmatrix}\begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 9 & 2 \\ 12 & 6 \end{bmatrix} \bmod 13$

$= \begin{bmatrix} 1266 & 488 \\ 1758 & 664 \end{bmatrix} \bmod 13 = \begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}$

Here, $p^{-1} = \begin{bmatrix} 9 & 2 \\ 12 & 6 \end{bmatrix}^{-1} \bmod 13 = \begin{bmatrix} 8 & 6 \\ 10 & 12 \end{bmatrix}$

Signature Generation

In this phase, the signature is generated for send a message i.e., for a given message $M = \begin{bmatrix} 9 & 2 \\ 12 & 6 \end{bmatrix}$

The person A computes hash function

$H\left(M\right) = \begin{bmatrix} 2^9 & 2^2 \\ 2^{12} & 2^6 \end{bmatrix}$ mod 13= $\begin{bmatrix} 5 & 4 \\ 1 & 12 \end{bmatrix}$.

A also chooses another random polynomial $r = 2x + 5$ and computes $r = \left(2\begin{bmatrix} 2 & 3 \\ 5 & 4 \end{bmatrix} + 5I\right) \bmod 13$

$= \begin{bmatrix} 9 & 6 \\ 10 & 0 \end{bmatrix}$ and the inverse of r is

$r^{-1} = \begin{bmatrix} 9 & 6 \\ 10 & 0 \end{bmatrix}^{-1} \bmod 13 = \begin{bmatrix} 0 & 4 \\ 11 & 7 \end{bmatrix}$.

Now, she computes

$l = r^{-1}q\,r = \begin{bmatrix} 0 & 4 \\ 11 & 7 \end{bmatrix}\begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 9 & 6 \\ 10 & 0 \end{bmatrix} \bmod 13$

$= \begin{bmatrix} 148 & 72 \\ 1524 & 456 \end{bmatrix} \bmod 13 = \begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}$

$n = p^{-1}H(M)\,l\,p$

$= \begin{bmatrix} 8 & 6 \\ 10 & 12 \end{bmatrix}\begin{bmatrix} 5 & 4 \\ 1 & 12 \end{bmatrix}\begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 9 & 2 \\ 12 & 6 \end{bmatrix} \bmod 13 = \begin{bmatrix} 6 & 0 \\ 3 & 11 \end{bmatrix}$

$$o = r^{-1} n\, r$$

$$= \begin{bmatrix} 0 & 4 \\ 11 & 7 \end{bmatrix} \begin{bmatrix} 6 & 0 \\ 3 & 11 \end{bmatrix} \begin{bmatrix} 9 & 6 \\ 10 & 0 \end{bmatrix} \bmod 13 = \begin{bmatrix} 2 & 7 \\ 6 & 2 \end{bmatrix}$$

$$t = r^{-1} n\, p$$

$$= \begin{bmatrix} 0 & 4 \\ 11 & 7 \end{bmatrix} \begin{bmatrix} 6 & 0 \\ 3 & 11 \end{bmatrix} \begin{bmatrix} 9 & 2 \\ 12 & 6 \end{bmatrix} \bmod 13 = \begin{bmatrix} 12 & 2 \\ 4 & 12 \end{bmatrix}$$

$$u = p^{-1} H(M)\, r$$

$$= \begin{bmatrix} 8 & 6 \\ 10 & 12 \end{bmatrix} \begin{bmatrix} 5 & 4 \\ 1 & 12 \end{bmatrix} \begin{bmatrix} 9 & 6 \\ 10 & 0 \end{bmatrix} \bmod 13$$

$$= \begin{bmatrix} 1454 & 276 \\ 2398 & 372 \end{bmatrix} \bmod 13 = \begin{bmatrix} 11 & 3 \\ 6 & 8 \end{bmatrix}$$

$$v = r^{-1} H(M)\, r$$

$$= \begin{bmatrix} 0 & 4 \\ 11 & 7 \end{bmatrix} \begin{bmatrix} 5 & 4 \\ 1 & 12 \end{bmatrix} \begin{bmatrix} 9 & 6 \\ 10 & 0 \end{bmatrix} \bmod 13$$

$$= \begin{bmatrix} 516 & 24 \\ 1838 & 372 \end{bmatrix} \bmod 13 = \begin{bmatrix} 9 & 11 \\ 5 & 8 \end{bmatrix}$$

Then A sends $(l,\ o,\ t,\ u,\ v)$ i.e., $\left(\begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 7 \\ 6 & 2 \end{bmatrix}, \begin{bmatrix} 12 & 2 \\ 4 & 12 \end{bmatrix}, \begin{bmatrix} 11 & 3 \\ 6 & 8 \end{bmatrix}, \begin{bmatrix} 9 & 11 \\ 5 & 8 \end{bmatrix} \right)$ to B as her signature.

Signature Verification

In this phase, the signature is verified by receiving the data from the first person. For this, after getting the signature which is generated by A, B will do the following.

$$w = t\, y^{-1} u = \begin{bmatrix} 12 & 2 \\ 4 & 12 \end{bmatrix} \begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 11 & 3 \\ 6 & 8 \end{bmatrix} \bmod 13$$

$$= \begin{bmatrix} 9 & 5 \\ 10 & 3 \end{bmatrix}$$

Here $y^{-1} = \begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}^{-1} \bmod 13 = \begin{bmatrix} 4 & 11 \\ 1 & 7 \end{bmatrix}$

Verifies that $l^{-1} v = \begin{bmatrix} 4 & 11 \\ 1 & 7 \end{bmatrix} \begin{bmatrix} 9 & 11 \\ 5 & 8 \end{bmatrix} \bmod 13$

$$= \begin{bmatrix} 91 & 132 \\ 44 & 67 \end{bmatrix} \bmod 13 = \begin{bmatrix} 0 & 2 \\ 5 & 2 \end{bmatrix}$$

$$o^{-1} w = \begin{bmatrix} 2 & 6 \\ 7 & 2 \end{bmatrix} \begin{bmatrix} 9 & 5 \\ 10 & 3 \end{bmatrix} \bmod 13$$

$$= \begin{bmatrix} 78 & 28 \\ 83 & 41 \end{bmatrix} \bmod 13 = \begin{bmatrix} 0 & 2 \\ 5 & 2 \end{bmatrix}$$

$$\therefore\ l^{-1} v = o^{-1} w$$

Hence B accepts the signature which is received from A is authenticated, otherwise the signature is rejected.

The above is an example of a proposed algorithm, which shows the correct ness of the algorithm. Next we are showing the flowchart for the above example, how it will work

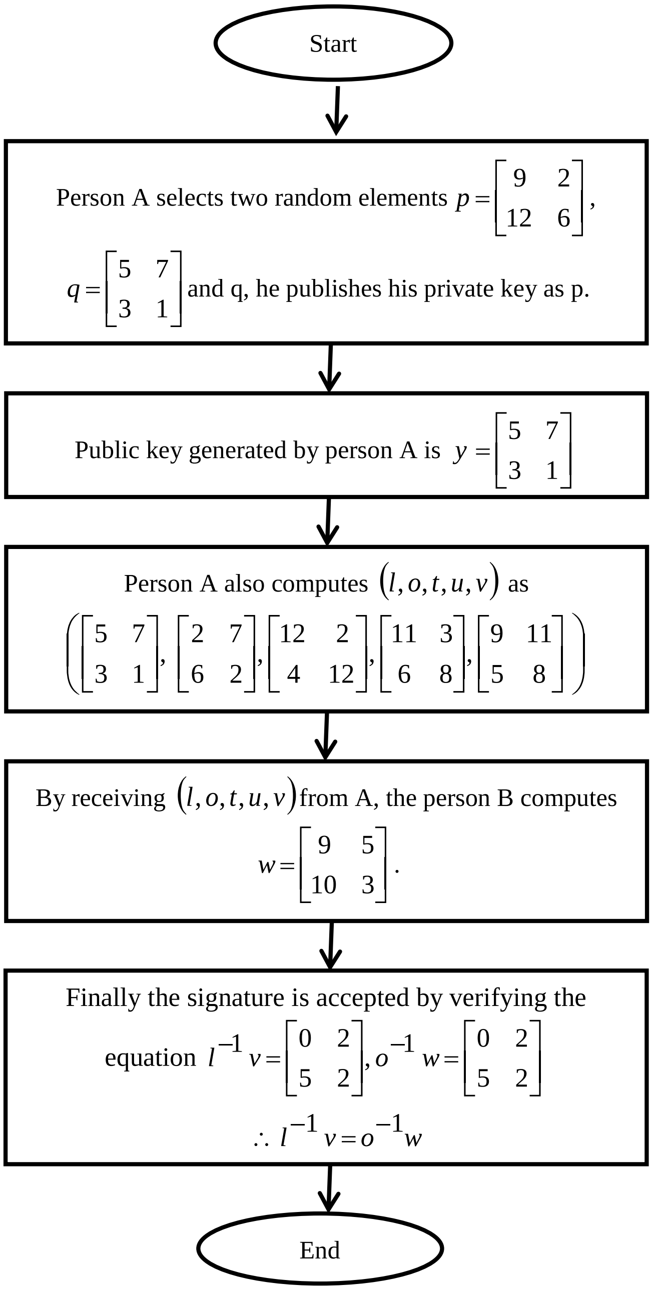

Start
Person A selects two random elements $p = \begin{bmatrix} 9 & 2 \\ 12 & 6 \end{bmatrix}$, $q = \begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}$ and q, he publishes his private key as p.
Public key generated by person A is $y = \begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}$
Person A also computes (l,o,t,u,v) as $\left(\begin{bmatrix} 5 & 7 \\ 3 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 7 \\ 6 & 2 \end{bmatrix}, \begin{bmatrix} 12 & 2 \\ 4 & 12 \end{bmatrix}, \begin{bmatrix} 11 & 3 \\ 6 & 8 \end{bmatrix}, \begin{bmatrix} 9 & 11 \\ 5 & 8 \end{bmatrix} \right)$
By receiving (l,o,t,u,v) from A, the person B computes $w = \begin{bmatrix} 9 & 5 \\ 10 & 3 \end{bmatrix}$.
Finally the signature is accepted by verifying the equation $l^{-1} v = \begin{bmatrix} 0 & 2 \\ 5 & 2 \end{bmatrix}, o^{-1} w = \begin{bmatrix} 0 & 2 \\ 5 & 2 \end{bmatrix}$
$\therefore l^{-1} v = o^{-1} w$
End

Figure 2. Flowchart of example for the proposed algorithm

SECURITY ANALYSIS AND RESULTS AND DISCUSSION

In this section, we are proving how the proposed scheme is secured with respect to other schemes with the help of security attacks. We test the signature scheme's security against four attacks: total break, data forgery on valid signature, signature repudiation, and existential forgery.[30-34]

Total Break

If the difficulty of generating the secret signature key from publicly available data is solved, a signature system is secure. The public verification data is inaccessible. This property is now used by everyone. It is determined by the intractable aspect of some computing problems arising from number or group theory. We utilized an intractable problem such as Conjugacy problem in this algorithm. Thus, we cannot find the secret key.

Data Forgery

Verifying the equation $l^{-1} v = o^{-1} w$ with forged data is not possible since M_f (or) $H\left(M_f\right)$ is presented in the structure of signature generation. As a result $l^{-1} v = o^{-1} w$, this is only true for the actual message and not for forged data. Therefore, invalid data cannot be signed with a valid signature.

Signature Repudiation

Assume that one can use a forgered signature $\left(l_f, o_f, t_f, u_f, v_f\right)$instead of the original message $\left(l, o, t, u, v\right)$ to replace and sign the message. Because the verification process includes $w = t y^{-1} u$, it is not possible. As a result, the non-repudiation property is ensured by this signature technique.

Existential Forgery

Assume that an attacker tries to sign a forged message. She could first replace the private key with some. Because double Conjugacy is intractable on non-commutative semi rings, she immediately gets a problem with the public key. As a result, it is impossible to create new valid signatures if the private key information is incorrect. So, an attacker will be unable to find forged signatures.

Comparison between hard problems and security analysis of different digital signatures on non-commutative structures.

Table 1: Comparison between hard problems and security attacks

Hard Problem/ Property	Integer Factorization Problem	Discrete Logarithm Problem	Conjugacy Problem	Double Conjugacy Problem	Reason
Total break	Secure	More secure	More secure	Adequate security	These results are proved based on strong mathematical logic.
Data forgery	Secure	Secure	More secure	Good security	
Signature Repudiation	Secure	Secure	Secure	Excellent security	
Existential forgery	Secure	Secure	Secure	Secure	

CONCLUSION

We developed a novel digital signature technique based on double Conjugacy over a non-commutative ring in this paper. The main idea behind our scheme is to use double Conjugacy over a non-commutative ring. We also demonstrated the signature scheme's strength by proving the confirmation theorem. Total break, data forgery, signature repudiation, and existential forgery are all prevented by the proposed signature system. We also used the Conjugacy problem to generate the keys for this signature scheme. As a result, this scheme is also secure against total failure.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

1. X. Lai, James L. Massey. Hash function based on block ciphers. *Advances in Cryptography-Euro crypt 92*. **1993**, 658, 55-70.
2. D. Poulakis. A Variant of Digital Signature algorithm, *Designs, Codes and Cryptography*. **2009,** 99-104.
3. J. Mo, H. Chen. A lightweight Secure User Authentication and Key Agreement Protocol for Wireless Sensor Networks. *Security and Communication Networks*. **2019**, 1-7.
4. S. Wei. A New Digital Signature Scheme Based on Factoring and Discrete logarithms. *Progress on Cryptography*. **2004**, 107-111.
5. T. El Gamal. A public key cryptosystem and a signature scheme based on discrete Logarithms, *Advances in Cryptography*. **2000**, 10-18.
6. E.S. Ismail, NMF Tahat, R.R. Ahmad. A new digital signature scheme based on factoring and discrete logarithms. *J. Mathematics Statistics*. **2008**, 222-225.
7. G.S.G.N Anjaneyulu, P.V. Reddy. Secured digital signature scheme using polynomials over non commutative division semirings. *Int. J. Computer Sci. Network Security*. **2008**, 278-284.
8. A. Raulynaitis, E. Sakalauskas, P. Tvarijonas. Key agreement protocol using conjugacy and discrete logarithm problems in group representation level. *Informatica*. **2007**, 115–124.
9. S. Vishnoi, V. Shrivastava. A new digital signature algorithm based on factorization and discrete logarithm problem. *Int. J. Computer Trends Technol*., **2012**, 3(4), 653-657.
10. S.W. Kim. The twisted Conjugacy problem for finitely generated free groups. *J. Pure Appl. Algebra*. **2016**, 220(4), 1281-1293.
11. N. Ghadbane. On Public key cryptosystem based on the word problem in a group. *J. Discrete Mathematical Sci. Cryptography*. **2022**, 1563-1568.
12. Bi, Wei, X. Jia, M. Zheng. A secure multiple elliptical curves digital signature algorithm for blockchain., *arXiv preprint arXiv:1808.02988*, **2018.**
13. S. Khatoon, S.M. Rahman, M. Alrubaian, A. Alamri. Privacy-Preserved, Provable Secure, Mutually Authenticated Key Agreement Protocol for Healthcare in a Smart City Environment. *IEEE*. **2019**, 47962-47971.
14. A.G. Reddy, A.K. Das, V. Odelu, A. Ahmad, J.S. Shin. A Privacy Preserving three- factor Authenticated Key Agreement Protocol for Client- Server Environment. *J. Ambient Intelligence Humanized Computing*. **2019**, 661-680.
15. N. Busom , R. Petrlic, F. Sebe, C. Sorge, M. Valls. Efficient smart metering based on homomorphic encryption, *Computer Commun.* **2016**, 95-101.
16. P. Balasubramanian, S. Ganapathy, A New Digital Signature Algorithm for Ensuring the Data Integrity in Cloud using Elliptic Curves, *Int. Arab J. Information Technol.*, **2021**, 180-190.
17. Q. Xie, DS. Wong, G. Wang, X. Tan, K. Chen, L. Fang. Provably Secure dynamic Id Based Anonymous Two-Factor Authenticated key

Exchange protocol with Extended security Model. *IEEE Trans Info Forensics Secur*. **2017**, 1382-92.

18. P. Liu, S. H. Shirazi, W. Liu, Y. Xie. PKAS: A Secure password based Key Agreement Scheme for the Egde Cloud. *Security and communication Networks*. **2021**, 1-10.
19. S. Iswariya, A.R. Rishivarman. An arithmetic technique for non abelin group cryptosystem. *Int. J. Computer Applications*. **2017**, 32-35.
20. L. Narendra Mohan, GSGN. Anjaneyulu New Key Agreement Protocol and Cryptosystem over ECC under SET Protocol Environment in E-Commerce. *J. Intelligent Engineering & Systems*. **2022**, 319-328
21. W. Diffie and M. Hellman. New Directions in Cryptography. *IEEE Transactions in Information Theory*. **1976**, 644-654.
22. V. Shpilrain, G. Zapata. Using decision problems in public key cryptography. *Groups-Complexity-Cryptol*. **2009**, 1(1), 33–49.
23. D. Wang, P. Wang. Offline dictionary attack on password authentication schemes using smart cards. *Information secuirty, Springer, Berlin*. **2015**, 221-237.
24. R. Madhusudhan, M. Hegde. Security Bound Enhancement of Remote User Authentication Using Smart Card, *J. Information Security Appl*. **2017,** 59-68.
25. I. Anshel, M. Anshel and D. Goldfeld. An algebraic method for public-key cryptography. *Math. Res. Lett.*. **1999,** 6, 287–291.
26. G. Mittal, S. Kumar, S. Narain, S. Kumar. Group ring based public key cryptosystems, *J. Discrete Mathematical Sci. Cryptography*. **2022**, 25(6), 1683-17029.
27. A. Pandey, I. Gupta. A new undeniable signature scheme on general linear group over group ring. *J. Discrete Math. Sci. Cryptography*. **2022**, 25(5), 1261-1273.
28. K.R. Blaney, A. Nikolaev. A PTIME solution to the restricted conjugacy problem in generalized Heisenberg groups. *Groups Complexity Cryptol*. **2016**, 8(1), 69–74.
29. D. Poulakis. A Variant of Digital Signature algorithm, *Designs, Codes and Cryptography*. **2009**, 99-104.
30. M.J. Craven, J.R. Woordward. Evolution of group theoretical cryptology attacks using hyper heuristics. *J. Mathematical Cryptology*. **2021**, 49-63.
31. S. Xiao, H. Wang, J. Zhang. New Digital Signature Algorithm Based on ECC and it's Application in Bit coin and IOT. *Int. J. High Performance Systems Architecture*. **2021**, 10(1), 20-31.
32. Z. Shao. Security of a new digital signature scheme based on factoring and discrete logarithms. *Int. J. Computer Math.*, **2005**, 82(10), 1215-1219.
33. S. Kumari, M.K. Khan, X. Li. An improved remote user authentication scheme with key agreement, *Computer Electronics Engineering*, **2014**, 1997-2012
34. L. Ham. Enhancing the security of El Gamal's signature scheme. IEEE Proceedings-Computer and Digital Techniques, **1995,** 142-145.