J. Integr. Sci. Technol. 2024, 12(6), 830

Article

Journal of Integrated
SCIENCE & TECHNOLOGY

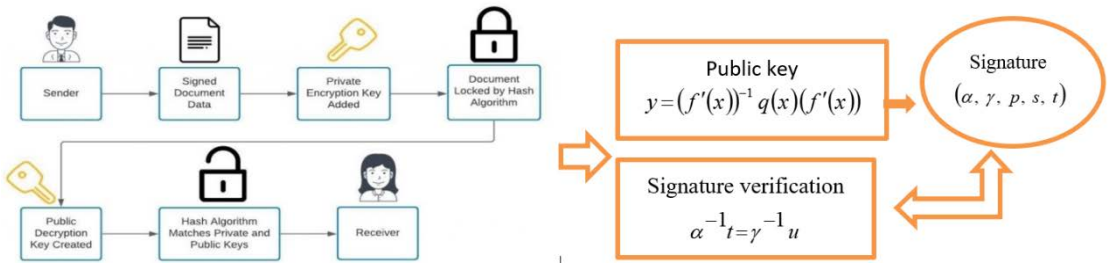
Novel Digital Signature scheme on Non-Commutative Rings using Differential Polynomials in conjugacy problem

V. Jalaja,[1*] L. Narendra Mohan,[2] Kotte Amaranadha Reddy,[3] B. Srinivasa Kumar,[4] K. Hemabala[1]

[1]Mathematics, Mohan Babu University (Erstwhile Sree Vidyanikethan Engineering College), Tirupathi, India. [2]Mathematics, Sri Venkateswara College of Engineering, Tirupathi, India. [3]Mathematics, Kalasalingam Academy of Research and Education, Tamilnadu, India. [4]Mathematics, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, India.

Received on: 09-Jan-2024 Accepted: 31-May-2024, and published on: 07-Jun-2024

ABSTRACT



A method for digital signatures ensures the security of messages sent between individuals. Several algorithms have been developed by focusing on individual challenging issues like conjugacy problem, discrete logarithm problem, and integer factorization problem. Though, it has been noted that these techniques are challenging to calculate in order to get at an appropriate solution. These days, the majority of algorithms are created by combining two challenging tasks. With a single challenging problem, we created an algorithm that deals comparable security. In this work, we provide a novel digital signature scheme that takes advantage of non-commutative rings characteristics. The digital signature is protected by the hardness of the conjugacy problem on non-commutative structures and also it is designed by using differential polynomials. We believe that conjugacy problem is NP-hard. The confirmation theorem was used to show the algorithm's strength. Security analysis was also explained.

Keywords: Conjugacy problem, Digital Signature, Differential polynomials, Non-Commutative Ring.

INTRODUCTION

The author of the communication can affix a code that serves as a signature to the message using an authentication technique called a digital signature. It satisfies the requirements of authenticity, integrity, and non-repudiation by acting as a handwritten signature. Paper documents are frequently authenticated with handwritten signatures. In the same way, a digital signature can be used to validate electronic documents.[1] A common idea for digital signatures is to establish a good working region, identify challenging issues inside this framework, develop a one-way function that references these challenging issues, and finally develop an algorithm. Rather than group theory, it is employed to address the unsolvable issues that are directly related to number theory.[2]

Diffie & Hellman (DH) used PKC for the first time in 1976. PKC's primary goal is to make symmetric-key cryptography and it is easier to use by eliminating the need for two separate keys in order for users to interact in confidence. The number of keys required for symmetric-key cryptography to be used in the case of n users exchanging secret data rises quickly with the number of users. Each user in PKC produces two keys: one that is meant be kept secret and the other that is public or open. When used for encryption, exposed key is referred to as "public key," and when used for decoding, secret key is referred to as "private key." In contrast to symmetric key cryptography, no key is shared here. PKC's recent noteworthy reach in this area.

The majority of techniques used today are based on solving discrete logarithm[3,15] and prime factorization problems together, yet each has unique drawbacks and weaknesses. The difficulty of resolving a number of complex theoretical problems is applied to modern encryption. These algorithms are safe as long as the problem they are based on remains secure.

*Corresponding Author: V. Jalaja
Tel: +91 94924 60994 Email: valisireddyjalaja0@gmail.com

Cite as: *J. Integr. Sci. Technol., 2024, 12(6), 830.*
URN:NBN:sciencein.jist.2024.v12.830

J. Mo et al.[2] used the key agreement protocol to explain a method for secure transmission. To transmit a message under this scheme, each member must create their own private key. When the algorithm is finished, both parties must confirm that a message is authentic.[2]

S. Vishnoi et.al.[1] offered an approach with the help of two challenging mathematical problems like prime factorization and discrete logarithm. Most algorithms only include one challenging problem such as the prime factorization problem or the discrete logarithm problem.[1] They clarified the various flaws and interruptions of the earlier algorithms. Additionally, they clarified the idea that attacking this technique would only be possible if both issues could be solved at the same time. Since the algorithm is built by taking many difficult issues, it is not feasible.

S. Kim[3] suggested a solution to the conjugacy problem for finitely produced free groups.[3] Some writers introduced this technique and built a backdoor system to circumvent the ECDSA.[4] The number of elliptic curves that can be chosen via this system is adjustable, however each elliptical curve's parameters must be specified.[5,20]

Khatoon et. al.[6] devised a plan that uses NKAP-ECDH-SET to provide high level security. Additionally, they offered the message's authentication and demonstrated the minimal calculation cost.[6]

A three-factor authenticated key agreement system that preserves privacy was developed by A.G. Reddy et.al.[8] for use in client-server environments. They used a special key agreement mechanism to create a scheme. They demonstrated that the algorithm's execution time is short in comparison to other algorithms by employing a unique key.[8]

A plan that uses the concept of double conjugacy problem in the smart meter system has been reported in the literature.[7,8] The double conjuggacy problem is employed safely in the algorithms creation and verification stages.[7,8]

A technique based on elliptic curves was created by Balasubramanian et. al.[9] to ensure data integrity in the cloud.[9] They built the previously mentioned algorithm, which uses elliptic curves, in a cloud database. Elliptic curve cryptography-based algorithms and their applications in Bitcoin and the Internet of Things were covered by Shuai Xiao et al.[12]

A secure password-dependent key agreement mechanism was presented by Liu et.al.[10]; the password key agreement process in elliptic curve cryptography was utilized in this paper. There are four phases to the algorithm: the initialization phase, the registration phase, the key authentication phase, and the accepting key phase.[10] S.Iswariya et.al., described an article title an arithmettic technique for non-abelian group cryptosystem. They constructed a cryptosystem on finite non-abelian groups in this paper. Compared to other public key cryptosystems, it works significantly faster because both encryption and decryption are based on non-commutative groups.[11]

Wang et.al.[14] and R.Madhusudhan et al.[13] exaplained the drawbacks of Ding's dynamic ID based remote user authentication scheme. They also identified, the implementation of Ding's scheme takes more cost compared to other methods. To overcome the above faults they introduced a scheme by preventing the drawbacks of Ding's scheme with less number of computational cost. [13-14]

K.R. Blaney et.al.[16] presented aa solution of conjugacy problem in generalized Heisenberg groups.[16] M.J. Craven et.al.[17] explained that the evolution of group theoretic crytology attacks using hyper-heuristics. This scheme is supported to implement in similar kinds of problems, which give the solution of cryptology problems over groups.[17]

A.Pandey and associates have suggested a novel undeniable signature system in a non-abelian group over group ring, the security of which depends on how hard it is to solve the factorization with discrete logarithm issue.[19] The essential idea of our solution is that, for a given set, we treated the Conjugacy problem as NP-hard. The conjugacy problem in non-commutative algebraic structure is an intractable problem.[21]

A CONJUGATION OF CRYPTOGRAPHIC ASSUMPTIONS OVER NON-COMMUTATIVE RING

A Conjugacy problem is the selection of two elements in a non-commutaitve group that are said to be conjugate to each other, for any two elements $x, y \in S$ if $z = y^{-1} x\, y$ for some $y \in S$. The Conjugacy problem is an equivalence relation, since it satisfies conditions reflexive, symmetric and transitive.

New digital signature scheme presented over non-commutaitve rings using differential polynomials

In this section, we describe the steps of the proposed technique and apply the proposed system to a set of matrices that we consider.[18,21] The method consists mainly of three stages: the creation of keys, the creation of signatures, and the verification of signatures. The public and private keys will generate during the key generation phase. The signature is generated at the signature generation stage and can be used as a code to guarantee the message's security; to access the message, the signature must be validated during the signature verification stage.

The steps which describe the algorithm are as follows.

Initial setup

Let $(R^*, +, .)$ be a non-commutative ring that helps as the foundation for our work organization. Let the message space be the definition for the cryptographic hash function H and is defined from R^* to the message space M $\left(i.e.,\ H : R^* \to M \right)$.

Key Generation

Let's say some one wishes to send a message and a document. Suppose A wants to send a message M. She then forwards it to the person for confirmation. For this, she chooses $f(x)\ \&\ q(x)$ two random polynomials are belongs to the set R^* and she computes $y = \left(f'(x) \right)^{-1} q(x)\ f'(x)$ and publishes her public key's are $y\ \&\ q$ and $f'(x)$ is her private key.

Signature Generation

The person A computes the following.

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

$$\alpha = \left(r'(x) \right)^{-1} q(x)\, r'(x)$$

$\beta = \left(f'(x)\right)^{-1} H(M)\, \alpha\ f'(x)$

$\gamma = \left(r'(x)\right)^{-1} \beta\, r'(x)$

$p = \left(r'(x)\right)^{-1} \beta\ f'(x)$

$s = \left(f'(x)\right)^{-1} H(M)\ r'(x)$

$t = \left(r'(x)\right)^{-1} H(M)\, r'(x)$

After that, the message $(\alpha,\ \gamma,\ p,\ s,\ t)$ is signed and forwarded to B for authentication and verification.

Signature Verification

After receiving a signature $(\alpha,\ \gamma,\ p,\ s,\ t)$, the person B verifying the signature will take the following action.

He makes calculations for this

$u = py^{-1}s$

B agrees to sign the document if and only if

$\alpha^{-1}t = \gamma^{-1}u$

Otherwise, the signature is rejected.

This flow chart provides an overview of the method mentioned above.

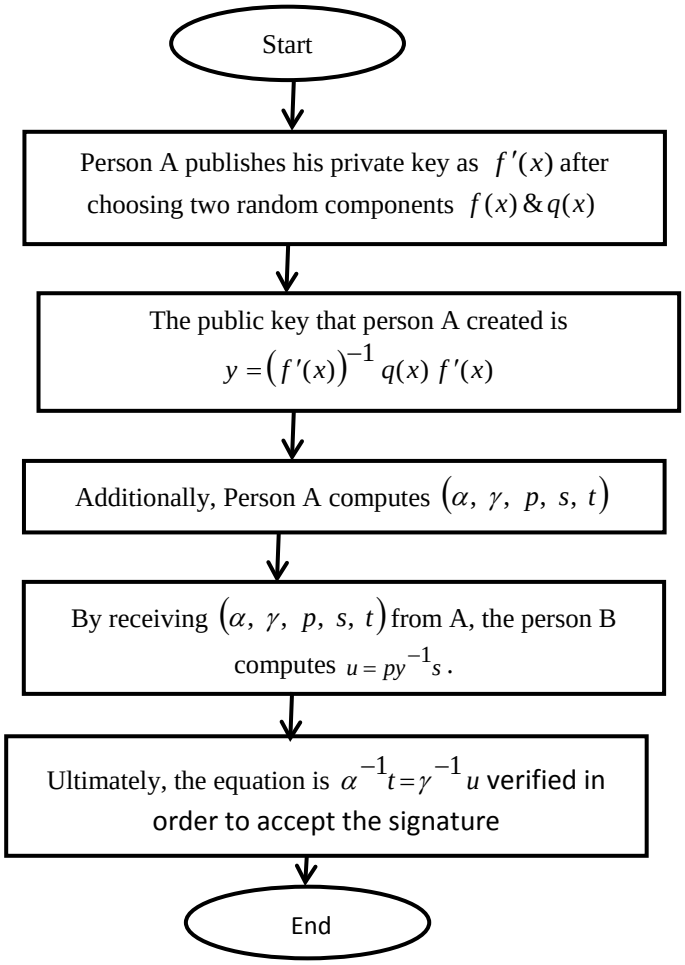


Figure 1. Flowchart for the proposed algorithm

CONFIRMATION THEOREM

In this section, we prove the confirmation theorem, which gives the strength of the suggested method. "The signature is always accepted as valid if the signature verification algorithm is followed," according to this theorem.

Proof:

In order to verify the algorithm, two individuals must compute the subsequent values.

$u = p\, y^{-1}s$

$= \left(r'(x)\right)^{-1}.\beta.f'(x).\left(f'(x)\right)^{-1}.\left(q(x)\right)^{-1}.f'(x).\left(f'(x)\right)^{-1}.H(M).r'(x)$

$u = \left(r'(x)\right)^{-1} \beta \left(q(x)\right)^{-1} H(M)\, r'(x)$

$\gamma^{-1}u = \left(\left(r'(x)\right)^{-1} \beta\, r'(x)\right)^{-1} \left(\left(r'(x)\right)^{-1} \beta \left(q(x)\right)^{-1} H(M)\, r'(x)\right)$

$= \left(r'(x)\right)^{-1} \beta^{-1} r'(x) \left(r'(x)\right)^{-1} \beta \left(q(x)\right)^{-1} H(M)\, r'(x)$

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

$\alpha^{-1}t = \left(\left(r'(x)\right)^{-1} q(x)\, r'(x)\right)^{-1}.\left(r'(x)\right)^{-1} H(M)\, r'(x)$

$= \left(r'(x)\right)^{-1}.\left(q(x)\right)^{-1}.r'(x).\left(r'(x)\right)^{-1}.H(M).r'(x)$

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

$\therefore\ \alpha^{-1}\, t = \gamma^{-1}u$

EXAMPLE

The digital signature scheme mentioned above is validated using a non-commutative matrix ring.

Initial setup

Let's say we select a matrix ring R^* and perform standard addition and multiplication operations on it. [27-29]

Define

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

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

Let cryptographic hash function H is a mapping from R^* to the message space M $\left(i.e., H : R^* \to M\right)$ and it is defined by $m_{ij} \to 2^{m_{ij}} \bmod p$ for $m_{ij} \in M_2\left(Z_p\right)$. We selected $p = 23$ and assessed every computation in the group that involved multiplication by 13.

Key Generation

In the phase of key generation, the individual A selects $x=\begin{bmatrix}2 & 3\\ 5 & 4\end{bmatrix}\in S$ and a random polynomial $f(x)=2x^3+4x^2+9x+11$ such that $f'(x)=6x^2+8x+9$.

So, $f'(x)=6\begin{bmatrix}2 & 3\\ 5 & 4\end{bmatrix}^2+8\begin{bmatrix}2 & 3\\ 5 & 4\end{bmatrix}+9\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\bmod 23$

$=\begin{bmatrix}139 & 132\\ 220 & 227\end{bmatrix}\bmod 23$

$f'(x)=\begin{bmatrix}1 & 17\\ 13 & 20\end{bmatrix}$ as her private key and then computes public key by randomly choosing $q(x)=3x^2+6x+1$.

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

$=\begin{bmatrix}70 & 72\\ 120 & 118\end{bmatrix}\bmod 23$

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

Then, $\left(f'(x)\right)^{-1}=\begin{bmatrix}1 & 17\\ 13 & 20\end{bmatrix}^{-1}\bmod 23$

$\left(f'(x)\right)^{-1}=\begin{bmatrix}11 & 1\\ 17 & 4\end{bmatrix}$

$\left(q(x)\right)^{-1}=\begin{bmatrix}1 & 3\\ 5 & 3\end{bmatrix}^{-1}\bmod 23$

$\left(q(x)\right)^{-1}=\begin{bmatrix}17 & 6\\ 10 & 21\end{bmatrix}$

$y=\left(f'(x)\right)^{-1}q(x)\,f'(x)$

$=\begin{bmatrix}11 & 1\\ 17 & 4\end{bmatrix}\begin{bmatrix}1 & 3\\ 5 & 3\end{bmatrix}\begin{bmatrix}1 & 17\\ 13 & 20\end{bmatrix}\bmod 23$

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

Signature Generation

This stage generates the signature for sending a message, or for a specific message $M=\begin{bmatrix}1 & 17\\ 13 & 20\end{bmatrix}$

The person A computes hash function

$H(M)=\begin{bmatrix}2^1 & 2^{17}\\ 2^{13} & 2^{20}\end{bmatrix}\bmod 23=\begin{bmatrix}2 & 18\\ 4 & 6\end{bmatrix}$.

A also chooses another random polynomial $g(x)=x^2+5x+3$ and computes $g'(x)=2x+5$

$=\left(2\begin{bmatrix}2 & 3\\ 5 & 4\end{bmatrix}+5I\right)\bmod 23$

$g'(x)=\begin{bmatrix}9 & 6\\ 10 & 13\end{bmatrix}$ and the inverse of $\left(g'(x)\right)^{-1}$ is

$\left(g'(x)\right)^{-1}=\begin{bmatrix}9 & 6\\ 10 & 13\end{bmatrix}^{-1}\bmod 23=\begin{bmatrix}20 & 12\\ 20 & 5\end{bmatrix}$.

Now, she computes

$\alpha=\left(g'(x)\right)^{-1}q(x)\,g'(x)=\begin{bmatrix}20 & 12\\ 20 & 5\end{bmatrix}\begin{bmatrix}1 & 3\\ 5 & 3\end{bmatrix}\begin{bmatrix}9 & 6\\ 10 & 13\end{bmatrix}\bmod 23$

$=\begin{bmatrix}1680 & 1728\\ 1155 & 1245\end{bmatrix}\bmod 23=\begin{bmatrix}1 & 3\\ 5 & 3\end{bmatrix}$

$\beta=\left(f'(x)\right)^{-1}H(M)\alpha\,f'(x)$

$=\begin{bmatrix}11 & 1\\ 17 & 4\end{bmatrix}\begin{bmatrix}2 & 18\\ 4 & 6\end{bmatrix}\begin{bmatrix}1 & 3\\ 5 & 3\end{bmatrix}\begin{bmatrix}1 & 17\\ 13 & 20\end{bmatrix}\bmod 23$

$=\begin{bmatrix}22516 & 15372\\ 36064 & 24552\end{bmatrix}\bmod 23$

$=\begin{bmatrix}22 & 8\\ 0 & 11\end{bmatrix}$

$\gamma=\left(g'(x)\right)^{-1}\beta\,g'(x)$

$=\begin{bmatrix}20 & 12\\ 20 & 5\end{bmatrix}\begin{bmatrix}22 & 8\\ 0 & 11\end{bmatrix}\begin{bmatrix}9 & 6\\ 10 & 13\end{bmatrix}\bmod 23$

$=\begin{bmatrix}6880 & 6436\\ 6110 & 5435\end{bmatrix}\bmod 23$

$=\begin{bmatrix}3 & 19\\ 15 & 7\end{bmatrix}$

$\gamma^{-1}=\begin{bmatrix}3 & 19\\ 15 & 7\end{bmatrix}^{-1}\bmod 23=\begin{bmatrix}14 & 8\\ 16 & 6\end{bmatrix}$

$$p = \left(g'(x)\right)^{-1} \beta\, f'(x)$$
$$= \begin{bmatrix} 20 & 12 \\ 20 & 5 \end{bmatrix} \begin{bmatrix} 22 & 8 \\ 0 & 11 \end{bmatrix} \begin{bmatrix} 1 & 17 \\ 13 & 20 \end{bmatrix} \bmod 23$$
$$= \begin{bmatrix} 4236 & 13320 \\ 3235 & 11780 \end{bmatrix} \bmod 23$$
$$= \begin{bmatrix} 4 & 3 \\ 15 & 4 \end{bmatrix}$$

$$s = \left(f'(x)\right)^{-1} H(M)\; g'(x)$$
$$= \begin{bmatrix} 11 & 1 \\ 17 & 4 \end{bmatrix} \begin{bmatrix} 2 & 18 \\ 4 & 6 \end{bmatrix} \begin{bmatrix} 9 & 6 \\ 10 & 13 \end{bmatrix} \bmod 23$$
$$= \begin{bmatrix} 2274 & 2808 \\ 3750 & 4590 \end{bmatrix} \bmod 23 = \begin{bmatrix} 20 & 2 \\ 1 & 13 \end{bmatrix}$$
$$t = \left(g'(x)\right)^{-1} H(M)\, g'(x)$$
$$= \begin{bmatrix} 20 & 12 \\ 20 & 5 \end{bmatrix} \begin{bmatrix} 2 & 18 \\ 4 & 6 \end{bmatrix} \begin{bmatrix} 9 & 6 \\ 10 & 13 \end{bmatrix} \bmod 23$$
$$= \begin{bmatrix} 5112 & 6144 \\ 4440 & 5430 \end{bmatrix} \bmod 23 = \begin{bmatrix} 6 & 3 \\ 1 & 2 \end{bmatrix}$$

Then A sends $(\alpha,\ \gamma,\ p,\ s,\ t)$ i.e.,

$$\left(\begin{bmatrix} 1 & 3 \\ 5 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 19 \\ 15 & 7 \end{bmatrix}, \begin{bmatrix} 4 & 3 \\ 15 & 4 \end{bmatrix}, \begin{bmatrix} 20 & 2 \\ 1 & 13 \end{bmatrix}, \begin{bmatrix} 6 & 3 \\ 1 & 2 \end{bmatrix}\right)$$ to B as her signature.

Signature Verification

In this stage, the data obtained from the initial respondent is used to validate the signature. For this, the following will be done once the signature produced by is received.

$$u = p\, y^{-1} s = \begin{bmatrix} 4 & 3 \\ 15 & 4 \end{bmatrix} \begin{bmatrix} 17 & 6 \\ 10 & 21 \end{bmatrix} \begin{bmatrix} 20 & 12 \\ 1 & 13 \end{bmatrix} \bmod 23$$
$$= \begin{bmatrix} 2047 & 1327 \\ 6074 & 2852 \end{bmatrix} \bmod 23$$
$$= \begin{bmatrix} 0 & 16 \\ 2 & 0 \end{bmatrix}$$

Verifies that $\alpha^{-1} t = \begin{bmatrix} 17 & 6 \\ 10 & 21 \end{bmatrix} \begin{bmatrix} 6 & 3 \\ 1 & 2 \end{bmatrix} \bmod 23$

$$= \begin{bmatrix} 108 & 63 \\ 81 & 72 \end{bmatrix} \bmod 23 = \begin{bmatrix} 16 & 17 \\ 12 & 3 \end{bmatrix}$$

$$\gamma^{-1} u = \begin{bmatrix} 14 & 8 \\ 16 & 6 \end{bmatrix} \begin{bmatrix} 0 & 16 \\ 2 & 0 \end{bmatrix} \bmod 23$$
$$= \begin{bmatrix} 16 & 224 \\ 12 & 256 \end{bmatrix} \bmod 23 = \begin{bmatrix} 16 & 17 \\ 12 & 3 \end{bmatrix}$$

$\therefore\ \alpha^{-1} t = \gamma^{-1} u$

B accepts the signature that has been obtained from A an authenticated source; if not, the signature is refused.

An example of a suggested algorithm that demonstrates the algorithm's correctness is provided above. Next, we'll demonstrate the aforementioned example's flowchart and how it operates.

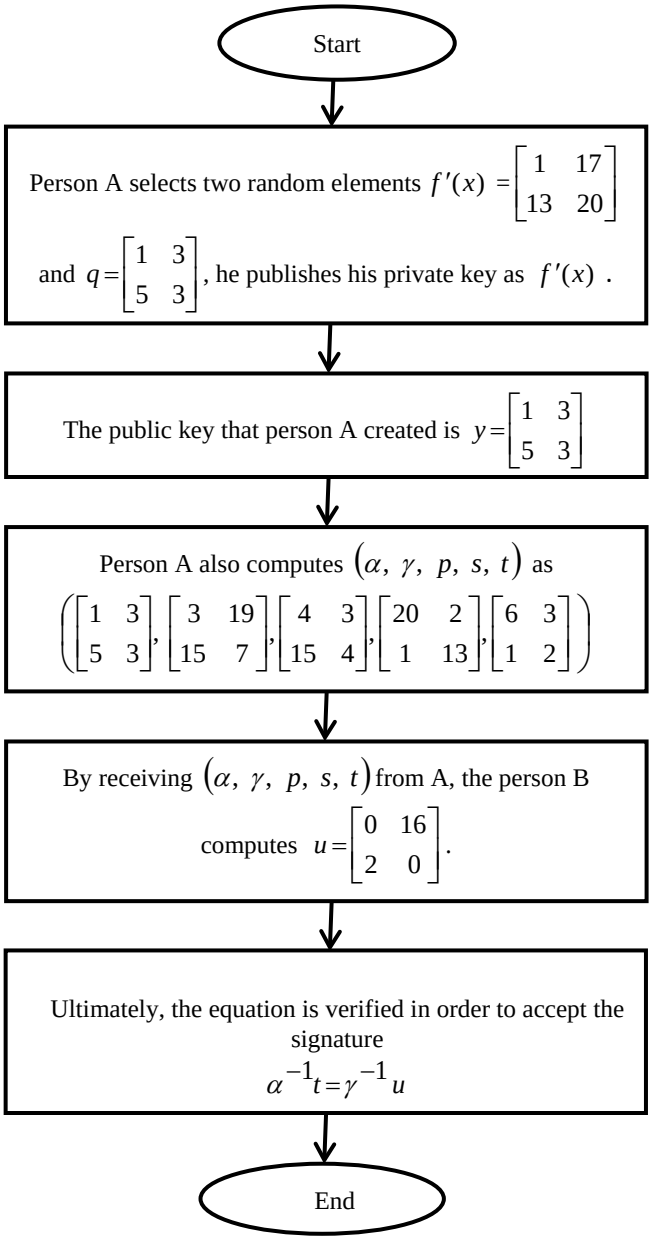


Figure 2. Flowchart of example for the proposed algorithm

SECURITY ANALYSIS, RESULTS AND DISCUSSION

In this section, we use security attacks to demonstrate how the suggested method is secure in comparison to alternative schemes. We evaluate the security of the signature system against four types

of attacks: existential forgery, signature repudiation, data forgery on valid signature, and total break.

Total Break

A signature system is secure if the problem of producing the secret signature key from publically accessible material is resolved. The verification data is not available to the public. Everyone now uses this property. It is based on the fact that certain computational issues originating from group or number theory are unsolvable. In this algorithm, we made use of an intractable problem like the conjugacy problem. So, we are unable to identify the secret key.

Data Forgery

Verification of the equation $\alpha^{-1}t=\gamma^{-1}u$ with fake data is not possible due to the representation of M_f (or) $H(M_f)$ in the signature generation structure. So this only applies to real messages, not fake data. As a result, a legitimate signature cannot be used to sign faulty data.

Signature Repudiation

Expect that one can utilize a fake signature $(\alpha_f, \gamma_f, p_f, s_f, t_f)$ rather than the first message $(\alpha, \gamma, p, s, t)$ to supplant and sign the message. Since the confirmation handle incorporates $u = py^{-1}s$, it isn't conceivable. As a result, the non-repudiation property is guaranteed by this signature strategy.

Existential Forgery

Suppose someone tries to sign a false communication. She could replace the private key with some first. On non-commutative semi rings, double conjugacy is unmanageable, therefore she encounters an issue with the public key right away. As a result, if the private key information is inaccurate, it is difficult to generate new, authorized signatures. Therefore, duplicate signatures will be impossible for an attacker to uncover.

The below table shows the details of the several digital signatures on non-commutative structures with hard challenges.[18]

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	Protected	More secure	More secure	Adequate security	These results are proved based on strong mathematical logic.
Data forgery	Protected	Protected	More secure	Good security	
Signature Repudiation	Protected	Protected	Protected	Excellent security	
Existential forgery	Protected	Protected	Protected	Protected	

CONCLUSION

In this research, we present differential polynomials in conjugacy issue over a non-commutative ring and provide a novel computerized signature system. Our technique relies on the conjugacy of differential polynomials over a non-commutative ring. Furthermore, we proved the confirmation theorem, which demonstrated the quality of the signature scheme. The proposed signature structure prevents existential forgery, total break, data forgery, and signature repudiation. For the purpose of creating the keys for this signature scheme, we also used the Conjugacy issue.This makes this approach even more secure against complete disruption.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

1. S. Vishnoi, V. Shrivastava. A new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem. *Int. J. Comput. Trends Technol.* **2012**, 3 (4), 653–657.
2. J. Mo, H. Chen. A Lightweight Secure User Authentication and Key Agreement Protocol for Wireless Sensor Networks. *Secur. Commun. Networks* **2019**, 2019, 1–17.
3. S.W. Kim. The twisted conjugacy problem for finitely generated free groups. *J. Pure Appl. Algebr.* **2016**, 220 (4), 1281–1293.
4. N. Ghadbane. On public key cryptosystem based on the word problem in a group. *J. Discret. Math. Sci. Cryptogr.* **2022**, 25 (6), 1563–1568.
5. G. Shankar, L.H. Ai-Farhani, P.A. Christy Angelin, P. Singh et.al. Improved Multisignature scheme for authenticity of digital document in digital forensics using Edward-curve Digital Signature Algorithm. *Security and Communication Networks*, **2023**, 2023(1), 2093407.
6. S. Khatoon, S.M.M. Rahman, M. Alrubaian, A. Alamri. Privacy-Preserved, Provable Secure, Mutually Authenticated Key Agreement Protocol for Healthcare in a Smart City Environment. *IEEE Access* **2019**, 7, 47962–47971.
7. V. Mai, I. Khalil. Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography. *Future Generation Computer Systems*, **2017**, 72, 327-338.
8. 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 Intell. Humaniz. Comput.* **2019**, 10, 661–680.
9. B.P. Kavin, S. Ganapathy. A new digital signature algorithm for ensuring the data integrity in cloud using elliptic curves. *Int. Arab J. Inf. Technol.* **2021**, 18 (2), 180–190.
10. P. Liu, S.H. Shirazi, W. Liu, Y. Xie. PKAS: A Secure Password-Based Key Agreement Scheme for the Edge Cloud. *Secur. Commun. Networks* **2021**, 2021, 1–10.
11. S. Iswariya, A. R. An Arithmetic Technique for Non-Abelian Group Cryptosystem. *Int. J. Comput. Appl.* **2017**, 161 (2), 32–35.
12. Q. Xie, D.S. Wong, G. Wang, et al. Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model. *IEEE Trans. Inf. Forensics Secur.* **2017**, 12 (6), 1382–1392.
13. R. Madhusudhan, M. Hegde. Security bound enhancement of remote user authentication using smart card. *J. Inf. Secur. Appl.* **2017**, 36, 59–68.
14. D. Wang, P. Wang. Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Information security, Springer, Berlin, **2015**; Vol. 7807, pp 221–237.
15. G. Mittal, S. Kumar, S. Narain, S. Kumar. Group ring based public key cryptosystems. *J. Discret. Math. Sci. Cryptogr.* **2022**, 25 (6), 1683–1704.

16. 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.
17. M. J.Craven, J.R. Woordward. Evolution of group theoretical cryptology attacks using hyper heuristics. *J. Math. Cryptol.* 49–63.
18. V. Jalaja, P.V. Kumar, R. Elumalai, G.S.G.N. Anjaneyulu. Differential polynomials on Non-Commutative Rings in Digital Signature scheme. *J. Integr. Sci. Technol.* **2023**, 11 (3), 526.
19. A. Pandey, I. Gupta. A new undeniable signature scheme on general linear group over group ring. *J. Discret. Math. Sci. Cryptogr.* **2022**, 25 (5), 1261–1273.
20. S. Xiao, H. Wang, J. Zhang. New digital signature algorithm based on ECC and its application in bitcoin and IoT. *Int. J. High Perform. Syst. Archit.* **2021**, 10 (1), 20–31.
21. V. Jalaja, G.S.G.N. Anjaneyulu, L.N. Mohan. New Digital Signature Scheme on Non-Commutative Rings using Double Conjugacy. *J. Integr. Sci. Technol.* **2023**, 11 (2), 471.