J. Integr. Sci. Technol. 2023, 11(3), 526

Article

Journal of Integrated
SCIENCE& TECHNOLOGY

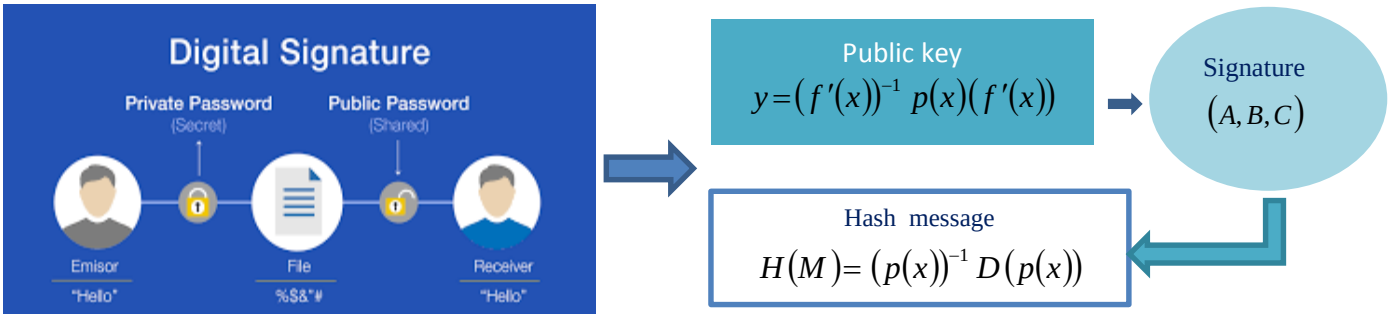
Differential polynomials on Non-Commutative Rings in Digital Signature scheme

V. Jalaja[1*], P. Vijay Kumar[2], Elumalai R[3], G.S.G.N. Anjaneyulu[3]

[1]Department of Mathematics, Sree Vidyanikethan Engineering College, Tirupathi, India. [2]Department of Mathematics, SAS, Vellore Institute of Technology, Chennai, India. [3]Department of Mathematics, Vellore Institute of Technology, Vellore, India.

Received on: 28-Dec-2022, Accepted and Published on: 26-Feb-2023

ABSTRACT



In general, digital signatures are based on difficult mathematical problems such as the discrete logarithmic problem, the Conjugacy problem, and the Integer factorization problem. In this article, authors propose a novel digital signature scheme using differential polynomials in Conjugacy problem over non-commutative structures. Initially, an algorithm on non-commutative rings in digital signatures have been generated and proved the confirmation theorem for the proposed algorithm. Finally, the signature algorithm has been evaluated for the security analysis.

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

INTRODUCTION

Now a days, Digital signature plays a vital role for sending messages from one another. These signatures are widely used in authentication and identification of protocols. Digital signatures enable users to sign a document using a signing key in such a way that all parties can verify the signature of the document using the corresponding public verification key. It also provides authenticity, integrity and non-repudiation for data. Most of the algorithms are designed in digital signatures, still some draw backs are there in those algorithms, that is with respect to security attacks.

Ismail et al.,[3] described a novel digital signature scheme based on factoring and discrete logarithms in 2008. This scheme involves a number of difficult problems, such as factoring and discrete logarithms. They combined these two problems in both signing and verifying equations, making it impossible for an attacker to obtain the information. They also proved the time complexity of the proposed signature generation is 1203Tmul+Th. Shao[4] Presented a scheme which is designed on the concepts factoring and discrete logarithms. Each user can use one private key and one public key in this scheme. We can demonstrate that their scheme is insecure because one of the attackers is capable of solving discrete logarithm or factorization problems. Anjaneyulu et al[11] proposed a signature scheme based on non-commutative division semi rings and polynomials. Initially they taken the non-commutative structure then they designed an algorithm.

In 2016, Seung Won Kim[5] presented a scheme using Conjugacy problem for finitely generated groups. Here, the group G is considered and the endomorphism of G is $\phi \in End(G)$. Logically, we can solve the endomorphism of G. N. Busom et.al[9] provided a tracking motive machine that preserves customer`s privateness through homomorphically aggregating the consumptions of all n participants of a neighbourhood. In 2017, Xie et.al.[6] presented a dynamic ID-based two factor AKE protocol. This scheme supports the revocation of smart card and updation of password without

*Corresponding Author: V Jalaja, Assistant Professor of Mathematics, Sree Vidyanikethan Engineering College, Tirupathi, India
Tel: +91-9492460994 Email: valisireddyjalaja0@gmail.com

Cite as: *J. Integr. Sci. Technol., 2023, 11(3), 526.*
URN:NBN:sciencein.jist.2023.v11.526

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

centralized storage of data. S. Iswarya et.al.[10] proposed an arithmetic technique for non-abelian group cryptosystem. Bi.Wei[8] proposed a multiple elliptic curves digital signature algorithm. In 2019, J.Mo et.al.[12] developed a lightweight security improved three factor authentication scheme for WSNS. This scheme is secured under the random oracle model. They also discussed the security analysis for the proposed scheme. Xin Wang et.al.[14] presented an advanced signature model for multivariate polynomial public key cryptosystem for key recovery. In this article they also explained recovery attack. The algorithm uses two pairs of public keys to design new public-key authentication conditions.

In 2020, Jalaja et.al.[2] presented a cryptosystem based on Conjugacy problem over non-commutative groups. They applied the proposed signature scheme in real life application such as smart meters. They designed a system that consists of customer's privacy by adding all consumptions of n members of a domain we get accumulate value. They also explained the comparison table for smart meters and electronic meters. In 2021, Balasubramanian et.al.,[1] developed an enhanced digital signature scheme for authenticating the sender and providing the integrity for the data. The algorithm is designed by using elliptic curves. That is, the signing and verification processes they used elliptic curves as a public key. They showed that the time for signing and verification of a document is less by compare to other methods. They also discussed the experiments and results for time complexity.

Shuai et.al.[7]showed that the proposed scheme is faster and more efficient in signing and verification than the original scheme. In 2022, R. kuang et.al.[13] proposed a new quantum safe digital signature algorithm. The proposed scheme is based on the modular arithmetic property that for a given element greater than equal to two. The time complexity of the proposed scheme is explained in the field of general linear group.

By reviewing all the above data, we designed an algorithm on digital signature on non-commutative rings using double conjugacy[15] and in continuous exploration, herein report the design of a novel digital signature by using differential polynomials in non-commutative structures for providing more security for the data.

The general digital signature algorithm working procedure is shown in the below flow chart.

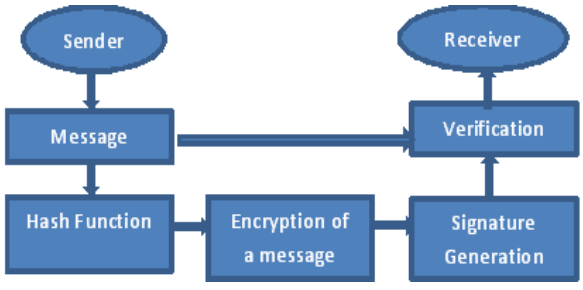


Figure.1 Flowchart for example of digital signature algorithm

MATHEMATICAL PRIMITIVES

Generally, most of the algorithms are designed by using more than one hard problem like discrete logarithm problem, Integer factorization problem, Conjugacy problem. Now we are presenting an algorithm by using single hard problem like Conjugacy problem without losing the security.

To define Conjugacy problem, first we have to consider the non-commutative group G, and take two elements $s,t \in G$ are called conjugate to each other if $r = t^{-1} s t$ for some $t \in G$.

PROPOSED DIGITAL SIGNATURE ALGORITHM

In this section, we are presenting the proposed digital signature scheme. Mainly the proposed scheme consists of three stages, namely Key generation, Signature generation and Signature verification. The steps which includes in the proposed algorithm is explained below.

Initial Setup

At the initial step, let us consider a non-commutative ring $\left(R^*, +, \cdot\right)$. We are taking this non-commutative ring as the platform for constructing new algorithm.

Consider hash function H is a mapping from R^* to the message $M\left(i.e., H : R^* \to M\right)$.

Key Generation

In this step, we will generate the key to send the document from one person to another. The first person A selects two random polynomials $f(x) \& p(x)$ from R^* and then she computes $y = \left(f'(x)\right)^{-1} p(x)\left(f'(x)\right)$, here $f'(x) = \frac{d}{dx}\left(f(x)\right)$ and publishes y and $p(x)$ are her public key's and $f(x)$ is her secret key.

Signature Generation

In this step, the first person will generate signature for the message and send to second person for verification.

For this, the first person computes the following

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

$$B = \left(p(x)\right)^{-1} A \left(p(x)\right)$$

$$C = \left(f'(x)\right)^{-1} B \left(f'(x)\right)$$

Then the first person sends C to the second person for verification and validation of the message.

Signature Verification

In this step, the second person receives the signature C from first person and then he computes

$$D = \left(p(x)y\right) C \left(p(x)y\right)^{-1}$$

Finally, the message is calculated by computing $H(M) = \left(p(x)\right)^{-1} D\left(p(x)\right)$.

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

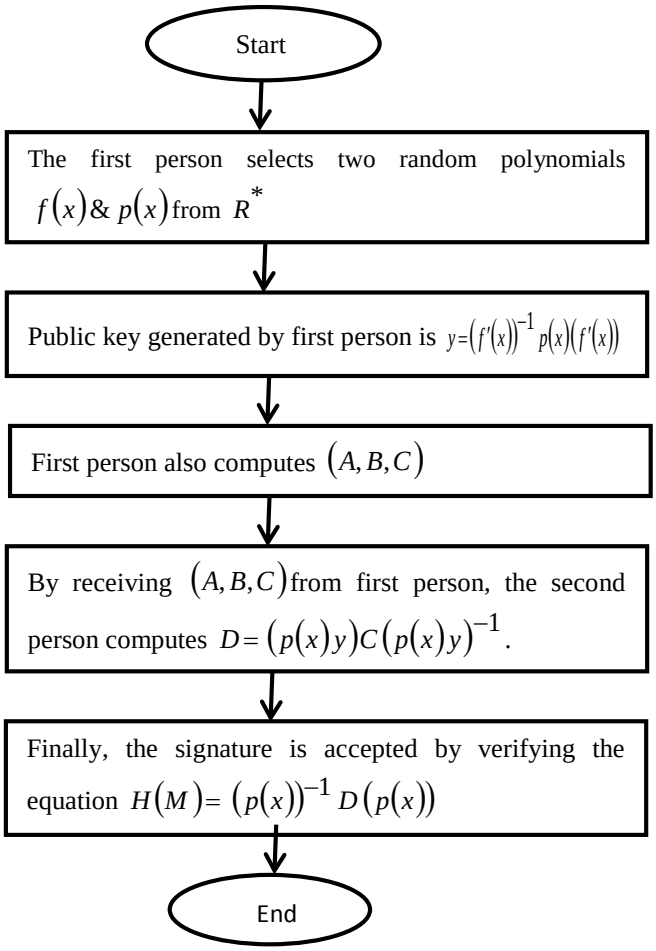


Figure 2. Flowchart for the proposed algorithm

CONFIRMATION THEOREM

We provide the strength of the proposed algorithm by proving the confirmation theorem in section. This theorem states that 'a signature is always accepted as valid if it follows the signature verification algorithms'.

Proof:

The first person calculates the following equations for verifying the algorithm.

$$H(M)=(p(x))^{-1}D(p(x))$$
$$=(p(x))^{-1}p(x)yCy^{-1}(p(x))^{-1}p(x)$$
$$=(f'(x))^{-1}p(x)f'(x)(f'(x))^{-1}Bf'(x)(f'(x))^{-1}(p(x))^{-1}(f'(x))$$
$$=(f'(x))^{-1}p(x)B(p(x))^{-1}(f'(x))$$
$$=(f'(x))^{-1}p(x)(p(x))^{-1}Ap(x)(p(x))^{-1}f'(x)$$
$$=(f'(x))^{-1}Af'(x)$$
$$=(f'(x))^{-1}f'(x)H(M)(f'(x))^{-1}f'(x)=H(M)$$

Example

We are verifying the above algorithm on matrices which are non-commutative.

Initial Setup:

We are choosing R^* is a 2×2 matrix division ring with the binary operations addition and multiplication. Define $M_2(Z_p)=\left\{\begin{bmatrix}p & q\\ r & s\end{bmatrix} / \ p,q,r,s\in Z_p \ for prime\ p\ and\ ps-qr\neq 0\right\}$ and $R^*=M_2(Z_p)\cup\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$ where p is prime. So, $(R^*,+,.)$ is a non-commutative division ring.

Let $H:R^*\to M$ be a cryptographic hash function which is a mapping from R^* to the message M and is defined by $m_{ij}\to 2^{m_{ij}} \bmod p$ for $m_{ij}\in M_2(Z_p)$. Here, we are selecting $p=23$ and calculating all calculations under multiplication modulo 23.

Key Generation:

The person 1 chooses $x=\begin{bmatrix}2 & 3\\ 5 & 4\end{bmatrix}\in M_2(Z_p)$ and a random polynomial $2x^3+4x^2+9x+7$ such that $f(x)=2x^3+4x^2+9x+7$ and computes $f'(x)=6x^2+8x+9\in R^*$

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

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

$$f'(x)=\begin{bmatrix}1 & 17\\ 13 & 20\end{bmatrix}$$

Similarly $(f'(x))'=\begin{bmatrix}1 & 17\\ 13 & 20\end{bmatrix}^{-1}\bmod 23=\begin{bmatrix}11 & 1\\ 17 & 4\end{bmatrix}$

And also selects $p(x)=3x^2+6x+1\in R^*$

$$p(x)=3\begin{bmatrix}2 & 3\\ 5 & 4\end{bmatrix}^2+6\begin{bmatrix}2 & 3\\ 5 & 4\end{bmatrix}+\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$
$$=\begin{bmatrix}70 & 72\\ 120 & 118\end{bmatrix}\bmod 23=\begin{bmatrix}1 & 3\\ 5 & 3\end{bmatrix}$$

$$(p(x))^{-1} = \begin{bmatrix} 1 & 3 \\ 5 & 3 \end{bmatrix}^{-1} \bmod 23 = \begin{bmatrix} 17 & 6 \\ 10 & 21 \end{bmatrix}$$

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

$$= \begin{bmatrix} 484 & 992 \\ 856 & 1889 \end{bmatrix} \bmod 23$$

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

Signature Generation:

Let the message $M = \begin{bmatrix} 1 & 17 \\ 13 & 20 \end{bmatrix}$

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

And

$$= \begin{bmatrix} 2 & 18 \\ 4 & 6 \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 17 \\ 13 & 20 \end{bmatrix}\begin{bmatrix} 2 & 18 \\ 4 & 6 \end{bmatrix}\begin{bmatrix} 11 & 1 \\ 17 & 4 \end{bmatrix} \bmod 23 = \begin{bmatrix} 4 & 21 \\ 8 & 4 \end{bmatrix}$$

$$B = \begin{bmatrix} 17 & 6 \\ 10 & 21 \end{bmatrix}\begin{bmatrix} 4 & 21 \\ 8 & 4 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 5 & 3 \end{bmatrix} \bmod 23 = \begin{bmatrix} 20 & 19 \\ 22 & 11 \end{bmatrix}$$

$$C = \begin{bmatrix} 11 & 1 \\ 17 & 4 \end{bmatrix}\begin{bmatrix} 20 & 19 \\ 22 & 11 \end{bmatrix}\begin{bmatrix} 1 & 17 \\ 13 & 20 \end{bmatrix} \bmod 23 = \begin{bmatrix} 20 & 4 \\ 1 & 11 \end{bmatrix}$$

Then the first person sends 'C' to second person for verification.

Signature Verification:

By taking 'C' from the first person, second person will do the following.

i.e., $D = (p(x)y)C(p(x)y)^{-1}$

$$p(x)y = \begin{bmatrix} 1 & 3 \\ 5 & 3 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 5 & 3 \end{bmatrix} \bmod 23 = \begin{bmatrix} 16 & 12 \\ 20 & 1 \end{bmatrix}$$

$$(p(x)y)^{-1} = \begin{bmatrix} 4 & 21 \\ 12 & 18 \end{bmatrix}$$

$$D = \begin{bmatrix} 16 & 12 \\ 20 & 1 \end{bmatrix}\begin{bmatrix} 20 & 4 \\ 1 & 11 \end{bmatrix}\begin{bmatrix} 4 & 21 \\ 12 & 18 \end{bmatrix} \bmod 23 = \begin{bmatrix} 0 & 12 \\ 5 & 8 \end{bmatrix}$$

Then the message $H(M)$ is verifies by the equation

$$H(M) = \begin{bmatrix} 17 & 6 \\ 10 & 21 \end{bmatrix}\begin{bmatrix} 0 & 12 \\ 5 & 8 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 5 & 3 \end{bmatrix} \bmod 23 = \begin{bmatrix} 2 & 18 \\ 4 & 6 \end{bmatrix}$$

Hence the second person gets the authenticated message from the first person.

An example of an above algorithm is described by using the below flow chart.

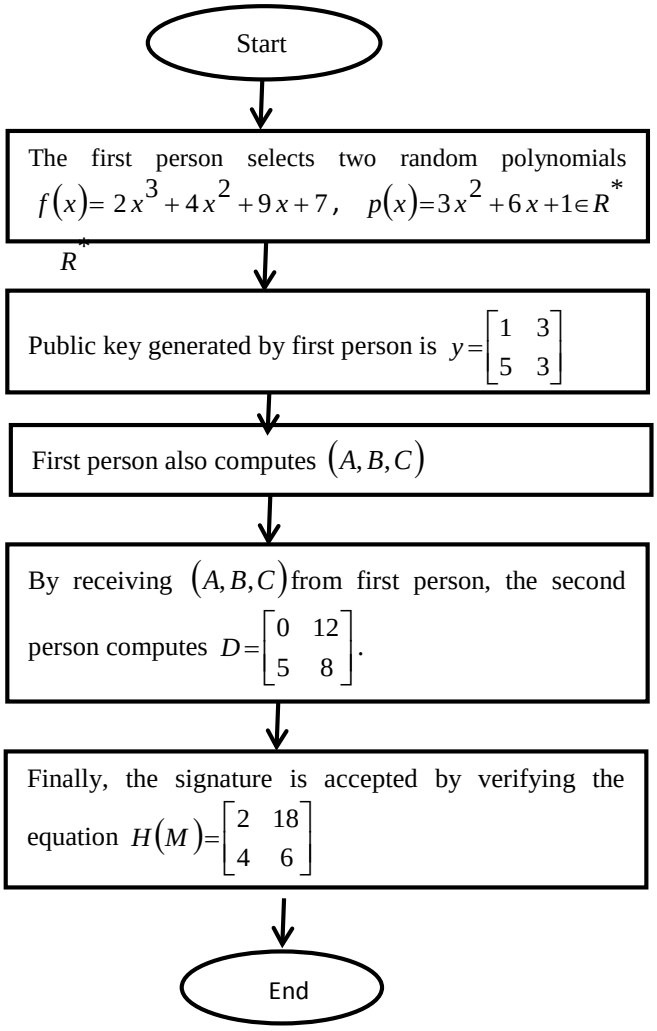


Figure 3. Flowchart for example of the proposed algorithm

SECURITY ANALYSIS AND RESULTS AND DISCUSSION

Here we are explaining the security analysis of the proposed signature scheme in terms of security attacks like Data forgery on valid signature and signature repudiation on valid data, authentication of a message and existential forgery.

Data Forgery

It is not possible for the attacker to perform a forgery attack without knowing the secret signature $f(x)$. Since $f(x)$ is involved in the signature generation and in the structure of Conjugacy with differentiation. To knowing $H(M)$ is not possible. Thus, the protocol satisfies its security against forgery attacks.

Signature Repudiation

Let us assume that anyone can use a forgered signature in place of original message. Then signature verification procedure is not possible, because it includes Conjugacy structure. i.e., verifying $D=\left(p(x)y\right)C\left(p(x)y\right)^{-1}$ is not possible. So, the non-repudiation property is ensured by this signature algorithm.

Authentication of a Message

Generally digital signature uses the authentication procedures to verify the validity of the signer. Each digital signature contains keys distributed by public key and private key that authorize the signer and creates the signature. The proposed signature is designed on double Conjugacy structure so, it is more secure. Also, the authorization is verified by the equation $D=\left(p(x)y\right)C\left(p(x)y\right)^{-1}$.

Existential Forgery

Suppose an attacker is trying to sign a forged message, first she could replace the private key with some. This is not possible, because Conjugacy is intractable on non-commutative rings and also the scheme is designed using derivatives of polynomials. So, the attacker gets a problem with the public key. It is impossible to create new signature if the private key information is not correct. Therefore an attacker will be unable to find forged signatures.

Table 1: Comparison between hard problems and security attacks[15]

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

CONCLUSION

We proposed a novel digital signature scheme using differential polynomials over non-commutative ring. This scheme is more secured because we introduced the derivative concept and the complete algorithm involves the derivatives of polynomials and also the hard mathematical problem like Conjugacy problem is involved. We also proved the confirmation theorem for giving strength to the algorithm. We also explained the security analysis like Data forgery, signature repudiation and existential forgery against to the proposed algorithm.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

1. Balasubramanian Prabhy Kavin, S. Ganapathy. A New Digital Signature Algorithm for Ensuring the Data Integrity in Cloud using Elliptic Curves. *Int. Arab J. Information Technol.*. **2021,** 18(2).
2. V. Jalaja, G.S.G.N Anjaneyulu. Expert smart metering system using homomorphic encryption with double Conjugacy problem. *JMCMS*. **2020**, 15(3), 19-35.
3. E.S. Ismail, N.M.F. Tahat, R.R. Ahmad. A New Digital Signature Scheme Based on Factoring and Discrete Logarithms. *JMS*. **2008**, 222-225.
4. Shao. Security of a new digital signature scheme based on factoring and discrete logarithms. *IJCM*. **2008**, 222-225.
5. S.W. Kim. The twisted Conjugacy problem for finitely generated free groups. *J. Pure and Applied Algebra*. **2016**. 220(4), 1281-1293.
6. Q. Xie, D.S.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.
7. S. Xiao, H. Wang, J. Zhang. New Digital Signature Algorithm Based on ECC and its Application in Bitcoin and IOT. *Int. J. High Performance Systems Architecture*. **2021**,10(1), 20-31.
8. B. Wei, X. Jia, M. Zheng. A secure multiple elliptical curves digital signature algorithm for block chain. *arXiv preprint arXiv:1808.02988*. **2018**.
9. N. Busom, R. Petrlic, F. Sebe, C. Sorge, M. Valls. Efficient smart metering based on homomorphic encryption. *Computer Commun*. **2016**, 95-101, 2016.
10. S. Iswarya, A.R. Rishivarman. An arithmetic Technique for Non-abelain Group Cryptosystem. *Int. J. Computer Appl.* **2017** 161(2).
11. G.S.G.N Anjaneyulu, P.V. Reddy. Secured digital signature scheme using polynomials over non commutative division semirings. *IJCSNS*. **2008,** 278-284.
12. J. Mo, H. Chen. A Lightweight Secure User Authentication and Key Agreement Protocol for Wireless Sensor Networks. *Security and Communication Networks*. **2019**, 1-17.
13. R. Kuang, M. Perepechaenko, M. Barbeau. A New Quantum-Safe Multivariate Polynomial Public Key Digital Signature Algorithm. *Scientific Reports 12*. **2022**.
14. X. Wang, B. Yang. An Improved Signature Model of Multivariate Polynomial Public Key Cryptosystem Against Key Recovery Attack. *Math. Biosci. Engin.*, **2019**, 16(6) 7734-7750.
15. 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.