OPEN ACCESS

European Journal of Engineering Science and Technology
ISSN 2538-9181

A Novel Public Key Cryptosystem and Digital Signatures

Saba Inam[1*], Shamsa Kanwal[1], Adnan Zahid[2], and Maria Abid[1]

[1] Fatima Jinnah Women University, the Mall, Rawalpindi, Pakistan
[2] Quaid-i-Azam University, Islamabad, Pakistan

ARTICLE INFO

Keywords:
Hash Function
Signature Scheme
Key Exchange Protocol
Complexity

ABSTRACT

In this article, we develop a new algebraic public key cryptosystem, which is based on generally non-commutative ring. Firstly, we define the polynomials over the non-commutative rings and then take it as underlying work structure. The hard problem of the scheme is the mixture of matrix discrete log problem under modular classes and polynomial symmetric decomposition problem. Using matrices of higher order and large modular classes resist the brute force and other well-known attacks exists in the literature. We also discuss the computational complexity of proposed scheme. On the other hand, we propose a signature scheme over a non-commutative division semiring. The key idea behind the signature scheme is that, for a given non-commutative division semiring, we build a polynomial and then implement digital signatures on multiplicative structure of semiring.

1. Introduction

Cryptography is very important need of today's world. Cryptography is a discipline of computer science in which the algorithms and security practices plays a central tool. But its foundation traditionally depends upon mathematics.

The first provoked though about the public key cryptography (PKC) was given by Diffie and Hellman (Diffie & Hellman, 1976). After that, many public key algorithms were proposed like RSA (Rivest et al., 1978), E

lGamal cryptosystem (ElGamal, 1985), elliptic curve cryptography (ECC) (Menezes, 1993) and the discrete logarithm problem (DLP) (Shor, 1997) and these schemes were considered to be secured. All the said schemes, systems and methods use some number theoretical and pure algebraic structures. Especially, we can say that RSA generally depends upon the structure of finite commutative groups and it works on invertible elements (units) of Z_n such that $n = p_1 p_2$; where p_1 and p_2 are randomly large prime numbers. However, the hard problem is to find these primes p_1 and p_2, because it depends on the factorization problem known as Integer Factorization Problem (IFP). But Peter Shor (Shor, 1995) proposed a quantum algorithm which can solve both IFP and DLP. In 2002, Stinson (Stinson, 2002) notice that mostly proposed PKC's eternally belongs to commutative group only whose security can be compromised by Shor's algorithm. Hence Lee and Goldreich advised that we do not put all the cryptographic protocols in one group. This is the reason to introduce a new field of cryptography known as non-commutative cryptography by (Lee, 2004). Then afterwards for various problems, key exchange protocols, encryption-decryption algorithms, authentication schemes were developed on non-commutative cryptosystem.

In the beginning, the generalization of the protocols for non-commutative cryptography was based on braid group. (Magyarik and Wagner, 1985) proposed a public key cryptography by

* Corresponding Author E-Mail Address: saba.inam@fjwu.edu.pk

using the elements of semigroup with undecidable word problem. But Birget et al. (Birget et al., 2006) told that the PKC proposed by Magyarik and Wagner actually did not depends on word problem and as a result they developed a new scheme which was based on finitely generated groups with hard problem. On braid group based cryptography, Anshel et al. (Anshel et al., 1999) proposed a key exchange protocol and the hard problem of this protocol was the difficulty of resolving equations over algebraic structures. In this research article, they mentioned that for PKC braid groups as a platform are a good choice. After this in 2000, Ko Lee et al. (Ko et al., 2000) developed a new key exchange protocol by using braid groups. The conjugacy search problem (CSP) is the underlying hard problem for this protocol. Furthermore, many successful schemes were proposed in this area by (Cha et al., 2001), (Anshel et al., 2003), (Dehornoy, 2004) and (Anshel et al., 2006). A review of group based cryptographic methods was discussed by Myasnokov et al. (Myasnikov et al., 2007) in the book "Group-based Cryptography". A new proposal is given by Cao et al. (Cao et al., 2007) on polynomials over non-commutative semi groups or rings. In 2016, S. Inam and R. Ali (Inam and Ali, 2016) developed a cryptosystem for which the underlying work structure is groupring and the hard problem is CSP. Another scheme is also formulated by S. Kanwal and R. Ali (Kanwal and Ali, 2016) by using non-commutative platform groups.

In this article, our contribution is in multidisciplinary scenario on polynomials over non-commutative rings on the cryptographic protocol regarding authentication, key exchange and encryption decryption algorithm. The rest of the article is organised as follows:

Section 2 is related with the basic definitions and cryptographic hard problems. In section 3, we propose digital signature and also give example to illustrate the given scheme. In section 4, we develop a new public key cryptosystem in which the polynomials over matrix ring is chosen as a platform. Section 5 deals with the security of proposed cryptosystem. In the last, section 6 discusses the conclusion of the proposed cryptosystem.

2. Preliminaries

In this section, we discuss some important definitions as well as the cryptographic hard problems which will be helpful in the next sections.

There are many cryptographic constructions for which we need functions which are easy to calculate but hard to invert, and one of the very well-known example is hash function. These functions are used as an application in digital signatures.

Definition 1 (Hash Function)

Hash function takes a message as an input and produce a hash code or hash value as an output. In simple words, we can say that applying hash on set of arbitrary finite length produce output of fixed length. The three secured desirable properties of hash function are as follows:

i. Given any hash output h, it is computationally infeasible to find an input message x, such that $H(x) = h$. This property is known as one way-ness.
ii. It is compulsory that the hash of the two different messages do no give the same answer in digital signature. This means that, to find $x \neq y$ with $H(x) = H(y)$ is computationally infeasible. This property is known as weak collision resistance.
iii. To find a pair (x, y) from $H(x) = H(y)$ is computationally infeasible. This property is known as strong collision resistance.

Hash functions are used as an application of cryptography which we call "data integrity".

Definition 2 (Matrix Discrete Logarithm Problem (MDLP))

For any group of matrices M, let $A, B \in M(F_q)$. To find an integer $d \in Z$ from the equation

$$A^d = B, \tag{1}$$

is known as matrix discrete logarithm problem.

Definition 3 (Decomposition Problem (DP))
Let us consider a non-commutative group G and $H \subseteq G$. Let $g_1, g_2 \in G$. To find the elements $h_1, h_2 \in H$ from the relation

$$g_1 = h_1 g_2 h_2, \tag{2}$$

is known as decomposition problem.
Definition 4 (Symmetric Decomposition Problem (SDP))
Let us consider a non-commutative group G. Let $g_1, g_2 \in G$ and $a, b \in Z$. To find the element $g_3 \in G$ from the relation

$$g_1 = g_3^a g_2 g_3^b, \tag{3}$$

is known as symmetric decomposition problem.
Definition 5 (Polynomial Symmetrical Decomposition Problem (PSDP))
Let R be a non-commutative ring. For any element $r \in R$, consider the set $S_r \subseteq R$ defined as

$$S_r = \{P(r) \mid P(x) \in Z_{>0}[x]\},$$

and $a, b \in Z$. Given two elements $g_1, g_2 \in R$, finding the element $h \in S_r$, where

$$g_2 = h^a g_1 h^b, \tag{4}$$

is known as polynomial symmetric decomposition problem.

3. Proposed Digital Signature Scheme

The digital signature scheme involves the main following steps:
3.1. Initialization
Let N be the product of two randomly large primes p *and* q, such that $N = pq$. Let $M_n(Z_N)$ be matrix ring and let $A, B \in M_n(Z_N)$. Choose $f(x) = a_0 + a_1 x^1 + a_2 x^2 + ... + a_{n_1} x^{n_1} \in Z_{>0}[x]$, be a positive integral coefficient polynomial. Calculate $P_1 = f(A) \bmod N$ and $Q_1 = f(B) \bmod N$.
3.2. Key Generation
Suppose Alice wants to communicate with Bob, then she signs and send message M to Bob for verification. She chooses $g(x) \in Z_{>0}[x]$, calculates $g(p_1) = N_1 \neq 0$ and $Y = \left(N_1^{m_1} Q_1 N_1^{m_2}\right) \bmod N$. Now Alice's private key is N_1 and her public key is the triplets as $(P_1, Q_1, Y) \in M_n(Z_N)$, where m_1 and m_2 are the integers.
3.3. Signature Generation
Alice performs the following steps to do the digital signatures:

i. Alice chooses a random polynomial $h(x) = c_0 + c_1 x^1 + c_2 x^2 + ... + c_{n_3} x^{n_3} \in Z_{>0}[x]$ and calculates $N_2 = h(P_1)$.
ii. For a message M, she computes hash of a message $H(M)$ and also calculates the following quantities as:
$\alpha = \left(N_2^{m_1} Q_1 N_2^{m_2}\right) \bmod N, \quad \beta = \left(N_1^{m_1} \{H(M)\alpha\} N_1^{m_2}\right) \bmod N, \quad \gamma = \left(N_2^{m_1} \beta N_2^{m_2}\right) \bmod N$
$\varphi = \left(N_2^{m_1} \beta N_1^{m_2}\right) \bmod N, \quad \psi = \left(N_1^{m_1} H(M) N_2^{m_2}\right) \bmod N, \quad \eta = \left(N_2^{m_1} H(M) N_2^{m_2}\right) \bmod N.$
iii. Hence Alice's signature on M is $(\alpha, \gamma, \varphi, \psi, \eta)$ and she sends it to Bob for verification and then accept it.

3.4. Verification

After receiving the signatures from Alice $(\alpha,\gamma,\varphi,\psi,\eta)$, Bob will perform the following steps: First, he computes $V=(\varphi Y^{-1}\psi)\bmod N$. He will accepts signatures if and only if

(5) $$(\alpha^{-1}\eta)\bmod N=(\gamma^{-1}V)\bmod N.$$

Otherwise, he rejects the signatures.

Remark: If there does not exist multiplicative inverse in $H(M)$**,** then verification has the form as $(\gamma\alpha^{-1}\eta)\bmod N=V\bmod N$**.**

Theorem:

If Bob verifies the signature scheme, then he always accepts $(\alpha,\gamma,\varphi,\psi,\eta)$ as a valid signature.

Proof: (Correctness)

Bob computes $(\alpha^{-1}\eta)\bmod N=\left(N_2^{m_1}Q_1N_2^{m_2}\right)^{-1}\left(N_2^{m_1}H(M)N_2^{m_2}\right)\bmod N$,

$$=\left(N_2^{-m_1}Q_1^{-1}H(M)N_2^{m_2}\right)\bmod N,$$
$$=\gamma^{-1}(\varphi Y^{-1}\psi)\bmod N,$$
$$=(\gamma^{-1}V)\bmod N.$$

Example

Here we will illustrate our signature scheme with the help of toy example. Let us consider two randomly primes $p=17$ and $q=11$, then $N=187$. Let

$$A=\begin{bmatrix}11 & 102\\ 121 & 101\end{bmatrix}\in M_2(Z_{187}) \quad \textit{and} \quad B=\begin{bmatrix}85 & 116\\ 169 & 89\end{bmatrix}\in M_2(Z_{187}),$$

$$f(x)=3x^3+4x^2+5x+6\in Z_{>0}[x].$$

Then we can find the following as:

$$P_1=f(A)=\begin{bmatrix}50 & 119\\ 110 & 155\end{bmatrix}\bmod 187 \quad \textit{and} \quad Q_1=f(B)=\begin{bmatrix}122 & 89\\ 41 & 9\end{bmatrix}\bmod 187.$$

For the key generation, Alice's chooses a polynomial $g(x)$ different from $f(x)$ as $g(x)=4x^2+5x+6\in Z_{>0}[x]$ and two integers $m_1=2,\ m_2=3$. She calculates her private key $N_1=g(P_1)=\begin{bmatrix}158 & 0\\ 55 & 15\end{bmatrix}\bmod 187$ and $Y=(N_1^2Q_1N_1^3)\bmod N=\begin{bmatrix}111 & 87\\ 19 & 42\end{bmatrix}\bmod 187$.

Hence Alice's public key is $(P_1,Q_1,Y)\in M_2(Z_{187})$.

For signature generation, first of all we have to introduce the hash function for a message M.

For any 2×2 matrix $K=\begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}$, hash is defined as $H(K)=\begin{bmatrix}2^{a_{11}} & 2^{a_{12}}\\ 2^{a_{21}} & 2^{a_{22}}\end{bmatrix}$.

If we choose a message $M=\begin{bmatrix}5 & 8\\ 81 & 56\end{bmatrix}$, then $H(M)=\begin{bmatrix}43 & 135\\ 2 & 86\end{bmatrix}\bmod 187$.

Next, she chooses different polynomial $h(x)=x^3+5x+1\in Z_{>0}[x]$ to find

$$N_2=h(P_1)=\begin{bmatrix}148 & 17\\ 55 & 19\end{bmatrix}\bmod 187,\ \alpha=(N_2^2Q_1N_2^3)\bmod N=\begin{bmatrix}44 & 171\\ 156 & 125\end{bmatrix}\bmod 187,$$

$$\beta = \left(N_1^2\{H(M)\alpha\}N_1^3\right)\bmod N = \begin{bmatrix} 50 & 182 \\ 84 & 136 \end{bmatrix}\bmod 187,$$

$$S = \left(N_2^2\beta N_2^3\right)\bmod N = \begin{bmatrix} 34 & 122 \\ 109 & 74 \end{bmatrix}\bmod 187,$$

$$\varphi = \left(N_2^2\beta N_1^3\right)\bmod N = \begin{bmatrix} 159 & 99 \\ 171 & 115 \end{bmatrix}\bmod 187,$$

$$\psi = \left(N_1^2 H(M) N_2^3\right)\bmod N = \begin{bmatrix} 17 & 4 \\ 73 & 123 \end{bmatrix}\bmod 187,$$

$$\eta = \left(N_2^2 H(M) N_2^3\right)\bmod N = \begin{bmatrix} 150 & 38 \\ 116 & 162 \end{bmatrix}\bmod 187.$$

Hence Alice sends all the above calculated quantities as a signature to Bob. For verification, Bob will go with the following steps:

He calculates $V = \left(\varphi Y^{-1}\psi\right)\bmod N = \begin{bmatrix} 66 & 5 \\ 164 & 10 \end{bmatrix}\bmod 187$, $\left(\alpha^{-1}\eta\right)\bmod N = \begin{bmatrix} 74 & 28 \\ 124 & 98 \end{bmatrix}\bmod 187$

and $\left(\gamma^{-1}V\right)\bmod N = \begin{bmatrix} 74 & 28 \\ 124 & 98 \end{bmatrix}\bmod 187.$

So we can easily see that the Bob verifies the signature and finally he accepts it.

4. Proposed Cryptosystem

Let us consider randomly two large primes p and q such that $N = pq$, a ring matrix $M_n(Z_N)$. Let $f(x) = a_0 + a_1x^1 + a_2x^2 + ... + a_nx^n \in Z_{>0}[x]$ be a positive integral coefficient polynomial. Now choose a matrix $A \in M_n(Z_N)$ and compute the base matrix $B = f(A) \bmod N$.

4.1. Key Generation

i. Bob chooses a secret random integer d_1 in the interval $[1, n-1]$.

ii. Next, he calculates $Q_1 = B^{d_1} \bmod N$. Make Q_1 public and d_1 secret.

iii. So, the private key is $(f(A), d_1)$ and public key is (Q_1, B).

4.2. Encryption

Let Alice wants to communicate with Bob, then she sends a message M as follows:

i. She chooses a random integer $d_2 \in [1, n-1]$ and computes $K = B^{d_2} \bmod N$.

ii. She calculates $K_1 = Q_1^{d_2} \bmod N$.

iii. Finally, she transmits the ciphertext pair (C, K), where C is defined as

$$C = \left(M * K_1\right)\bmod N.$$

4.3. Decryption

On receiving the ciphertext from Alice, Bob decrypts the message as follows:

First, he computes $K_2 = (K)^{d_1} \bmod N$. Finally he calculates to get the original plaintext back.

$$M = \left(C * K_2^{-1}\right)\bmod N,$$

Example:

Let us give an example which helps us to explain our proposed cryptosystem. For this consider two randomly large primes $p = 29$ and $q = 11$ such that $N = 319$, a polynomial $f(x) = 3x^3 + 4x^2 + 7x + 9 \in Z_{>0}[x]$ and a matrix $A = \begin{bmatrix} 112 & 45 & 66 \\ 203 & 288 & 6 \\ 300 & 9 & 12 \end{bmatrix} \in M_3(Z_{319})$.

Hence the base matrix is $B = f(A) = \begin{bmatrix} 40 & 214 & 92 \\ 15 & 87 & 257 \\ 230 & 63 & 204 \end{bmatrix} \bmod 319$.

For key generation, Bob chooses $d_1 = 167,\ 2 \le d_1 \le 319$ and find

$$Q_1 = \begin{bmatrix} 40 & 214 & 92 \\ 15 & 87 & 257 \\ 230 & 63 & 204 \end{bmatrix}^{167} \bmod 319 = \begin{bmatrix} 131 & 216 & 131 \\ 286 & 111 & 230 \\ 14 & 42 & 211 \end{bmatrix} \bmod 319.$$

For encryption, Alice randomly picks $d_2 = 216,\ 2 \le d_1 \le 319$ and calculates

$$K = \begin{bmatrix} 40 & 214 & 92 \\ 15 & 87 & 257 \\ 230 & 63 & 204 \end{bmatrix}^{216} \bmod 319 = \begin{bmatrix} 84 & 247 & 210 \\ 160 & 291 & 128 \\ 44 & 0 & 223 \end{bmatrix} \bmod 319,$$

$$K_1 = \begin{bmatrix} 131 & 216 & 131 \\ 286 & 111 & 230 \\ 14 & 42 & 211 \end{bmatrix}^{216} \bmod 319 = \begin{bmatrix} 24 & 214 & 210 \\ 303 & 77 & 304 \\ 77 & 220 & 185 \end{bmatrix} \bmod 319.$$

Now Alice wants to communicate with Bob, so she presents a message M as

$$M = \begin{bmatrix} 56 & 231 & 87 \\ 123 & 86 & 145 \\ 311 & 98 & 3 \end{bmatrix} \in M_3(Z_{319}).$$

$$C = (M * K_1) \bmod N = \begin{bmatrix} 56 & 231 & 87 \\ 123 & 86 & 145 \\ 311 & 98 & 3 \end{bmatrix} * \begin{bmatrix} 24 & 214 & 210 \\ 303 & 77 & 304 \\ 77 & 220 & 185 \end{bmatrix} \bmod 319,$$

$$C = \begin{bmatrix} 200 & 104 & 146 \\ 300 & 87 & 6 \\ 66 & 111 & 276 \end{bmatrix} \bmod 319.$$

Then she transmits the ciphertext (C, K) to Bob.

When Bob receives the pair of ciphertext pair, he will first find

$$K_2 = (K)^{d_1} \bmod N = \begin{bmatrix} 84 & 247 & 210 \\ 160 & 291 & 128 \\ 44 & 0 & 223 \end{bmatrix}^{167} \bmod 319,$$

$$K_2 = \begin{bmatrix} 24 & 214 & 210 \\ 303 & 77 & 304 \\ 77 & 220 & 185 \end{bmatrix} \bmod 319.$$

Finally he gets original plaintext message after calculating

$$\left(C * K_2^{-1}\right) \bmod N = \begin{bmatrix} 200 & 104 & 146 \\ 300 & 87 & 6 \\ 66 & 111 & 276 \end{bmatrix} * \begin{bmatrix} 24 & 214 & 210 \\ 303 & 77 & 304 \\ 77 & 220 & 185 \end{bmatrix}^{-1} \bmod 319,$$

$$\left(C * K_2^{-1}\right) \bmod N = \begin{bmatrix} 56 & 231 & 87 \\ 123 & 86 & 145 \\ 311 & 98 & 3 \end{bmatrix} \bmod 319,$$

$$= M$$

5. The computational Complexity of proposed cryptosystem

The computationally complexity of discrete logarithm problem computing is compared with the matrix discrete logarithm problem for encryption and decryption is as follows:

- *Discrete Logarithm Problem:*

i. Let us consider the size of input plaintext message units be n_1.

ii. The computing complexity of $\beta = \alpha^k \bmod p$ is:

$$T(\beta) = T(\alpha^k) = O(\log n_1),$$

arithmetic (multiplication) operation, using Fast Exponentiation Algorithm [ ] . Then

$$T(\alpha^k) = O(\log^3 n_1) \text{- bit operations.}$$

- *Matrix Discrete Logarithm Problem:*

i. Let us consider the size of input plaintext message units be n_1 and the size of base matrix be n_2.

ii. The computing complexity of $A_1 = A_2^{\,k} \bmod N$ is:

$$T(A_1) = T(A_2^k) = O(\log n_1),$$

using Repeated-Square and Multiplication Algorithm, then

$$T(A_2^k) = O(n_2^2 \log n_1), \text{ multiplication operation,}$$
$$T(A_2^k) = O(n_2^2 \log^3 n_1) \text{-bit operations.}$$

6. Security Analysis

First we will talk about the security analysis of signature scheme. For this, let us consider that an active attacker can obtain, remove, alter/forge and retransmit the message which Alice sends to Bob. Let us denote that altered/forged data by D_f .Here we discuss three main attacks on signature scheme that is data altering/forgering on signatures, signature repudiation on valid data.

Let us assume that an attacker replaces the original plaintext message M by forged message M_f . He tries to satisfy the Equation (refer with: Eq. 5) which is impossible because message is only involved in the signature generation not in the verification scheme. Hence Equation (refer with: Eq. 5) only true for original plaintext massage. Without extracting signatures, data forgery is not possible. The next attempt is to try to find M_f for $H(M)$. As we assume that hash is cryptographically secure, so by using M_f for hash is also impossible. Hence it is concluded that a forged data can't be signed with valid signature.

Now Alice's strategy is to refuse the recognition of signatures on the valid data. So the valid signature $(\alpha, \gamma, \varphi, \psi, \eta)$ can be forged by the cryptanalyst and she can sign a plaintext message

M with the forged signature as $(\alpha_f, \gamma_f, \varphi_f, \psi_f, \eta_f)$ and then the verification procedure is as follows:

$$V = (\varphi_f Y^{-1} \psi_f) \bmod N,$$
$$= \left(N_2^{m_1} \beta N_1^{m_2}\right)_f \left(N_1^{m_1} Q_1 N_1^{m_2}\right)^{-1} \left(N_1^{m_1} H(M) N_2^{m_2}\right)_f \bmod N,$$
$$= \left(N_2^{m_1} \beta N_1^{m_2}\right)_f \left(N_1^{-m_2} Q_1^{-1} N_1^{-m_1}\right) \left(N_1^{m_1} H(M) N_2^{m_2}\right)_f \bmod N.$$

Since $\left(N_1^{m_2}\right)_f \left(N_1^{-m_2}\right) \neq I$ and also $\left(N_1^{m_1}\right)_f \left(N_1^{-m_1}\right) \neq I$, where I is the identity matrix in the multiplcative division semiring. Hence we conclude that $\left(\alpha^{-1}\eta\right)_f \bmod N \neq \left(\gamma^{-1}V\right)_f \bmod N$. Hence, this ensures us non-repudiation in our proposed signature scheme.

Here we note that the proposed signature scheme is constructed on the non-commutative division semiring which is based on the polynomial symmetric decomposition problem. We believe that PSDP is intractable on non-commutative division semiring. Without proper knowledge of private keys the construction of new signature scheme is impossible. As a result, cryptanalyst is not able to compute forged signature.

The security of the proposed cryptosystem depends upon the different factors like the number N, the choice of the polynomial, the order of the matrices and matrix discrete logarithm problem.

Matrix cryptography depends upon the difficulty of solving MDLP, and it gives us the equal security for a far smallest bit size. Matrix multiplication is complicated and time consuming, hence the complexity increases with the choice of matrices of higher order. The intractability and complexity is increased with the choice of the polynomial and size of base matrix. To find the inverses in large modulo N becomes more difficult.

7. Conclusion

This manuscript is basically divided into two main parts. In the first part (Section 3), we propose the digital signatures and also verify its correctness. The key idea is that, we choose a random polynomial and for any $A \in M_n(Z_N)$, we have N_1. A cryptanalyst has no way to identify a polynomial $g(x) \in Z_{>0}[x]$ such that $N_1 \neq 0$, even he has infinite computation power. Hence there is a negligible probability to trace the exact private key because the scheme is based on intractability of PSDP. The proposed signature scheme is sound.

On the other hand, in the next part (Section 4) we develop a novel public key cryptosystem based on polynomials over non-commutative rings with detailed example. In matrix cryptography, the computational advantages are the use of the shortest key length which reduces all the calculation with secure systems. The MDLP is more complicated than DLP and ECDLP, because if the matrix size is increased, the complexity of matrix operations also increased. Hence we can say that our proposed scheme gives us good measures of safety.

References

Anshel, I., Anshel, M. and Goldfeld, D. (1999). "An algebraic method for public-key cryptography," *Mathematical Research Letters 6*, pp. 287-291.

Anshel, I., Anshel, M. and Goldfeld, D. (2003). "Non-abelian key agreement protocols," *Discrete Applied Mathematics- Special issue on the 2000 com2MaC*, vol. 130, pp. 3-12.

Anshel, I., Anshel, M. and Goldfeld, D. (2006). "A linear time matrix key agreement protocol over small finite fields," *Applicable Algebra in Engineering, Communication and Computing*, vol. 17, pp. 195-203.

Birget, J. C., Magliveras, S. S. and Sramka, M. (2006). "On public key cryptosystems based on combinatorial group theory," *Tatra Mountains Mathematical Publications*, vol. 33, pp. 137-148.

Cao, Z., Dong, X. and Wang, L. (2007). "New public key cryptosystems using polynomials over non-commutative rings," *Journal of Cryptology-IACR*, vol. 9, pp. 1-35.

Cha, J. C., Ko, K. H. Lee, S. J. Han, J. W. and Cheon, J. H. (2001). "An efficient implementation of braid groups," *in Advances in Cryptology-ASIACRYPT 2001*, C. Boyd, vol. 2248 of Lecture Notes in Computer Science, pp.144-156, Springer, Berlin, Germany.

Dehornoy, P. (2004). "Braid-based cryptography," *Contemporary Mathematics*, vol. 360, pp. 5-33.

Diffie, W. and Hellman, M. (1976). "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, pp. 644–654.

ElGamal, T. (1985). "A public key cryptosystem and a signature scheme based on Discrete Logarithms", *IEEE Transactions on Information Theory*, vol. 31, pp. 469-472.

Inam S. and Ali, R. (2018). "A new ElGamal-like cryptosystem based on matrices over groupring," *Neural Computing and Applications*, vol. 29, pp. 1279-1283.

Kanwal S. and Ali, R. (2018). "A cryptosystem with noncommutative platform groups," *Neural Computing and Applications*, vol. 29, pp. 1273-1278.

Ko, K. H. Lee, S. J. Cheon, J. H. Han, J. H. Kang, J. S. and Park, C. (2000). "New public-key cryptosystems using Braid groups," *CRYPTO '00 Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*, pp. 166-183.

Lee, E. (2004). "Braid groups in Cryptology," *ICICE Transactions on Fundamentals*, vol. 87, pp. 986–992.

Menezes, A. (1993). "*Elliptic Curve Public Key Cryptosystems*", The Springer International Series in Engineering and Computer Science, 1st ed., Springer US.

Myasnikov, A. G., Shpilrain, V. and Ushakov, A. (2007). "*Group-Based Cryptography*," Advanced Courses in Mathematics-CRM Barcelona, 1st ed., Birkhauser Basel.

Peter, W. S. (1994). "Algorithms for quantum computation: discrete logarithms and factorings," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134.

Rivest, R. L., Shamir, A. and Adleman, L. (1978). "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126.

Shor, P. W. (1997). "Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, pp. 1484-1509.

Magyarik, R. and Wagner, N. R. (1985). "A public key cryptosystem based on the word problem," *Workshop on the Theory and Application of Cryptographic Techniques CRYPTO 1984: Advances in Cryptology*, vol. 196, pp. 19-36.