A New Digital Signature Scheme Using Tribonacci Matrices

S.C. Gupta
Department of Mathematics,
Central Institute of Plastics Engg. & Tech.,
Raipur, Chhattisgarh, India

Manju Sanghi
Department of Applied Mathematics,
Rungta College of Engineering &Tech.,
Bhilai, Chhattisgarh, India
Email: manjusanghi13 [AT] gmail.com

Abstract- Achieving security is the most important goal for any digital signature scheme. The security of RSA, the most widely used signature is based on the difficulty of factoring of large integers. The minimum key size required for RSA according to current technology is 1024 bits which can be increased with the advancement in technology. Representation of message in the form of matrix can reduce the key size and use of Tribonacci matrices can double the security of RSA. Recently M. Basu et.al introduced a new coding theory called Tribonacci coding theory based on Tribonacci numbers, that are the generalization of the Fibonacci numbers. In this paper we present a new and efficient digital signature scheme using Tribonacci matrices and factoring.

Keywords- Digital signature, RSA, Fibonacci numbers, Tribonacci numbers, Tribonacci matrices.

I. INTRODUCTION

Increased use of Internet and data communication has increased the problem of authentication and confidentiality of data. Digital Signatures [1], [2] are one of the most important cryptographic primitives which provide the path for the solution of these problems. The concept of digital signatures was introduced by Diffie and Hellman in 1976. In a digital signature scheme, the signer uses private (secret) key to sign the messages and any one can verify it using signer's public key. The security of these signatures is based on the intractability of difficult mathematical problems like factorization and DLP. RSA [3] is the first and widely accepted signature scheme which is based on the factoring of integers. The security of RSA is based on large prime numbers which are usually 2048 bits long which would correspond to a decimal digit of 617 digits. Thereafter many signature schemes have been proposed by various researchers and almost in all the schemes the message to be signed is represented as an integer and their security is based on the difficulty of either factoring of integers or discrete logarithm problem. However, the security of these schemes is still a problem to be tackled. Currently, we find many new schemes [4], [5], [6], [7], [8] designed by using algebraic structures, linear groups, non-abelian groups like matrices and polynomials which are claimed to be more secure and efficient than the existing schemes. It is observed that the size of keys and storage space can be reduced by representing the plain text message as a matrix [9], [10],[11] without compromising the security. In [12] Bani et.al proposed a new kind of digital signature scheme using golden matrices which is a fast signature and can be used for protection of digital signals. Recently M. Basu et al. [13] introduced a new coding theory called Tribonacci coding theory based on Tribonacci matrices that are the generalization of Fibonacci numbers. They found that the correct ability of their method exceeds the correct ability of Fibonacci numbers and all well-known correcting codes. Motivated by this we propose a digital signature scheme based on Tribonacci matrices and factoring. Representation of a message in the form of matrix reduces the key size and use of

Tribonacci matrices adds to the security to the algorithm.

The rest of the paper is organized as follows. In Section 2 we briefly describe the basic concepts of Tribonacci numbers and Tribonacci matrix and their properties along with some theorems without proof (one may refer to [13] for details). In Section 3 we propose the new digital signature scheme followed by a simple example in Section 4. Section 5 explains the performance evaluation of the proposed scheme and finally the paper is concluded in Section 5.

II. TRIBONACCI NUMBERS AND TRIBONACCI MATRIX

The well-known Fibonacci numbers [14],[15],[16] F_n (n = 0, ±1, ±2, ±3, ...) are given by the recurrence relation

$$F_n = F_{n-1} + F_{n-2},\ n \geq 2 \qquad (2.1)$$

with the initial terms $F_0 = 0$, $F_1 = 1$

The Tribonacci numbers t_k (k = 0, 1, 2, 3....) are the generalization of the Fibonacci numbers [4] and are defined by the recurrence relation

$$t_k = t_{k-1} + t_{k-2} + t_{k-3},\ k \geq 3 \qquad (2.2)$$

where $t_0 = t_1 = 0$, $t_2 = 1$

The Tribonacci negative numbers t_{-k} (k = 1, 2, 3....) satisfies the recurrence relation

$$t_{-k} = \begin{vmatrix} t_{k+1} & t_{k+2} \\ t_k & t_{k+1} \end{vmatrix} \qquad (2.3)$$

where $t_0 = t_1 = 0$, $t_2 = 1$

Tribonacci numbers t_k (k = 0, ± 1, ± 2, ± 3....) are generated by the recurrence relations (2.2) and (2.3) as given in Table 1.

The limit $\alpha = \lim_{k\to\infty} \frac{t_k}{t_{k-1}}$ exists called Tribonacci constant and is the one and only real root of the equation $x^3 - x^2 - x - 1 = 0$. The value of α = 1.83928675. Tribonacci numbers t_k and the Tribonacci constant α both play an important role in the construction of Tribonacci coding theory.

In [13] the authors define the Tribonacci matrix T of order 3 as

$$T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} t_3 & t_2 + t_1 & t_2 \\ t_2 & t_1 + t_0 & t_1 \\ t_1 & t_0 + t_{-1} & t_0 \end{pmatrix} \qquad (2.4)$$

Such that ***det T*** = 1

The inverse of T is defined as

$$T^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & -1 \end{pmatrix} \qquad (2.5)$$

$$\begin{pmatrix} t_0^2 - t_{-1}t_1 & t_{-1}t_2 - t_0t_1 & t_1^2 - t_0t_2 \\ t_1^2 - t_0t_2 & t_0t_3 - t_1t_2 & t_2^2 - t_1t_3 \\ t_0t_2 + t_{-1}t_2 - t_1^2 - t_0t_1 & t_1^2 + t_1t_2 - t_0t_3 - t_{-1}t_3 & t_1t_3 + t_0t_3 - t_2^2 - t_1t_2 \end{pmatrix}$$

Such that ***det*** T^{-1} = det T = 1.

K	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10
T_k	7	5	-8	4	1	-3	2	0	-1	1	0	0	1	1	2	4	7	13	24	44	81

Table 1. Tribonacci numbers t_k

Also,

$$T^2 = \begin{pmatrix} 2 & 2 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} t_4 & t_3 + t_2 & t_3 \\ t_3 & t_2 + t_1 & t_2 \\ t_2 & t_1 + t_0 & t_1 \end{pmatrix} \quad (2.6)$$

Such that ***det*** $T^2 = 1$

and

T^{-2} =

$$\begin{pmatrix} t_1^2 - t_0 t_2 & t_0 t_3 - t_1 t_2 & t_2^2 - t_1 t_3 \\ t_2^2 - t_1 t_3 & t_1 t_4 - t_2 t_3 & t_3^2 - t_2 t_4 \\ t_1 t_3 + t_0 t_3 - t_2^2 - t_1 t_2 & t_2^2 + t_2 t_3 - t_1 t_4 - t_0 t_4 & t_2 t_4 + t_1 t_4 - t_3^2 - t_2 t_3 \end{pmatrix}$$

(2.7)

Such that ***det*** T^{-2} =1.

The following theorems are proved by induction in [13].

Theorem 2.1

$$\text{If } T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$T^k = \begin{pmatrix} t_{k+2} & t_{k+1} + t_k & t_{k+1} \\ t_{k+1} & t_k + t_{k-1} & t_k \\ t_k & t_{k-1} + t_{k-2} & t_{k-1} \end{pmatrix} \quad (2.8)$$

Theorem 2.2

$$\text{If } T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

T^{-k} =

$$\begin{pmatrix} t_{k-1}^2 - t_{k-2} t_k & t_{k-2} t_{k+1} - t_{k-1} t_k & t_k^2 - t_{k-1} t_{k+1} \\ t_k^2 - t_{k-1} t_{k+1} & t_{k-1} t_{k+2} - t_k t_{k+1} & t_{k+1}^2 - t_k t_{k+2} \\ t_{k-1} t_{k+1} + t_{k-2} t_{k+1} - t_k^2 - t_{k-1} t_k & t_k^2 + t_k t_{k+1} - t_{k-1} t_{k+2} - t_{k-21} t_{k+2} & t_k t_{k+2} + t_{k-1} t_{k+2} - t_{k+1}^2 - t_k t_{k+1} \end{pmatrix} (2.9)$$

Properties of Tribonacci matrix are

1. $T^k = T^{k-1} + T^{k-2} + T^{k-3}$
2. $T^k T^t = T^t T^k = T^{k+t}$ (k, t = 0, ±1, ±2, ±3....)
3. *det* $T^k = 1$.

III. NEW DIGITAL SIGNATURE SCHEME

In this section a new digital signature scheme based on factoring and Tribonacci matrices is proposed. The initial message is represented in the form of a square matrix of order 3 and the modulus n is selected such that the determinant of the matrix and modulus n are relatively prime. Then, N = $(p^3\text{-}1)\ (q^3\text{-}1)$ is calculated which gives the number of matrices relatively prime to n which is similar to Ø(n) = (p-1) (q-1) in RSA. Tribonacci matrix T^k is taken as the signature matrix and the inverse Tribonacci matrix T^{-k} as the verification matrix. The scheme involves the following steps:

Key generation

1. Randomly select two large primes p, q and compute the modulus n = p.q.

2. Calculate N = (p^3-1) (q^3-1) which gives the number of matrices that are relatively prime to n.
3. Select random integer e, 1< e < N such that e and N are relatively prime ie. gcd(e, N) =1.
4. Compute d = e^{-1} mod N where 1 < d < N and ed ≡ 1 mod N.
5. Public and private keys are now e and d respectively.

Signature generation

1. Represent the message M in the form of a square matrix of order 3 as

$$M = \begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix}$$

   with all the elements under mod n where n = pq and the determinant of M is relatively prime to n, i.e. gcd (|M|, n) = 1.
2. Compute α = T^k, k being a secret key and T being the Tribonacci matrix.
3. Compute the Signature S = M^d mod n.α.
4. Signature is now (S, α)

Signature Verification

1. Compute α^{-1}
2. Verify V = $[S\alpha^{-1}]^e$ mod n = M mod n.

Let us Suppose

$$M= \begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix}$$

$$M^d = \begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix}^d$$

$$= \begin{bmatrix} c_1 & c_2 & c_3 \\ c_4 & c_5 & c_6 \\ c_7 & c_8 & c_9 \end{bmatrix}$$

Signature S = M^d.α

= M^d T^k

$$= \begin{bmatrix} c_1 & c_2 & c_3 \\ c_4 & c_5 & c_6 \\ c_7 & c_8 & c_9 \end{bmatrix} \begin{pmatrix} t_{k+2} & t_{k+1}+t_k & t_{k+1} \\ t_{k+1} & t_k+t_{k-1} & t_k \\ t_k & t_{k-1}+t_{k-2} & t_{k-1} \end{pmatrix}$$

$$= \begin{bmatrix} c_1t_{k+2}+c_2t_{k+1}+c_3t_k & c_1(t_{k+1}+t_k)+c_2(t_k+t_{k-1})+c_3(t_{k-1}+t_{k-2}) & c_1t_{k+1}+c_2t_k+c_3t_{k-1} \\ c_4t_{k+2}+c_5t_{k+1}+c_6t_k & c_4(t_{k+1}+t_k)+c_5(t_k+t_{k-1})+c_6(t_{k-1}+t_{k-2}) & c_4t_{k+1}+c_5t_k+c_6t_{k-1} \\ c_7t_{k+2}+c_8t_{k+1}+c_9t_k & c_7(t_{k+1}+t_k)+c_8(t_k+t_{k-1})+c_9(t_{k-1}+t_{k-2}) & c_7t_{k+1}+c_8t_k+c_9t_{k-1} \end{bmatrix}$$

$$= \begin{bmatrix} s_{11} & s_{12} & s_{13} \\ s_{21} & s_{22} & s_{23} \\ s_{31} & s_{32} & s_{33} \end{bmatrix} \quad (3.1)$$

where

$$s_{11} = c_1t_{k+2}+c_2t_{k+1}+c_3t_k \quad (3.2)$$

$$s_{12} = c_1(t_{k+1}+t_k)+c_2(t_k+t_{k-1})+c_3(t_{k-1}+t_{k-2}) \quad (3.3)$$

$$s_{13} = c_1t_{k+1}+c_2t_k+c_3t_{k-1} \quad (3.4)$$

$$s_{21} = c_4t_{k+2}+c_5t_{k+1}+c_6t_k \quad (3.5)$$

$$s_{22} = c_4(t_{k+1}+t_k)+c_5(t_k+t_{k-1})+c_6(t_{k-1}+t_{k-2}) \quad (3.6)$$

$$s_{23} = c_4t_{k+1}+c_5t_k+c_6t_{k-1} \quad (3.7)$$

$$s_{31} = c_7t_{k+2}+c_8t_{k+1}+c_9t_k \quad (3.8)$$

s_{32} =

$$c_7(t_{k+1}+t_k)+c_8(t_k+t_{k-1})+c_9(t_{k-1}+t_{k-2}) \qquad (3.9)$$

$$s_{33} = c_7t_{k+1}+c_8t_k+c_9t_{k-1} \qquad (3.10)$$

Verification

V = [Sα^{-1}]^e mod n

= [S(T^k)$^{-1}$]^e mod n = [ST^{-k}]^e mod n.

$$=\left(\begin{bmatrix} s_{11} & s_{12} & s_{13} \\ s_{21} & s_{22} & s_{23} \\ s_{31} & s_{32} & s_{33} \end{bmatrix}\begin{pmatrix} t_{k-1}^2-t_{k-2}t_k & t_{k-2}t_{k+1}-t_{k-1}t_k & t_k^2-t_{k-1}t_{k+1} \\ t_k^2-t_{k-1}t_{k+1} & t_{k-1}t_{k+2}-t_kt_{k+1} & t_{k+1}^2-t_kt_{k+2} \\ t_{k-1}t_{k+1}+t_{k-2}t_{k+1}-t_k^2-t_{k-1}t_k & t_k^2+t_kt_{k+1}-t_{k-1}t_{k+2}-t_{k-21}t_{k+2} & t_kt_{k+2}+t_{k-1}t_{k+2}-t_{k+1}^2-t_kt_{k+1} \end{pmatrix}\right)^e$$

$$=\begin{bmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{bmatrix}^e \qquad (3.11)$$

where

v_{11} = s_{11} $(t_{k-1}^2-t_{k-2}t_k)$+ s_{12} $(t_k^2-t_{k-1}t_{k+1})$+

s_{13} $(t_{k-1}t_{k+1}+t_{k-2}t_{k+1}-t_k^2-t_{k-1}t_k)$ (3.12)

v_{12} = s_{11}($t_{k-2}t_{k+1}-t_{k-1}t_k$) + s_{12}($t_{k-1}t_{k+2}-t_kt_{k+1}$

) + s_{13}($t_k^2+t_kt_{k+1}-t_{k-1}t_{k+2}-t_{k-21}t_{k+2}$ (3.13)

v_{13} = s_{11}($t_k^2-t_{k-1}t_{k+1}$) + s_{12}($t_{k+1}^2-t_kt_{k+2}$)+

s_{13}($t_kt_{k+2}+t_{k-1}t_{k+2}-t_{k+1}^2-t_kt_{k+1}$) (3.14)

v_{21}= s_{21} $(t_{k-1}^2-t_{k-2}t_k)$+ s_{22} $(t_k^2-t_{k-1}t_{k+1})$+

s_{23} $(t_{k-1}t_{k+1}+t_{k-2}t_{k+1}-t_k^2-t_{k-1}t_k)$ (3.15)

v_{22} = s_{21}($t_{k-2}t_{k+1}-t_{k-1}t_k$) + s_{22}($t_{k-1}t_{k+2}-t_kt_{k+1}$

) + s_{23}($t_k^2+t_kt_{k+1}-t_{k-1}t_{k+2}-t_{k-21}t_{k+2}$)(3.16)

v_{23} = s_{21}($t_k^2-t_{k-1}t_{k+1}$) + s_{22}($t_{k+1}^2-t_kt_{k+2}$)+ s_{23}(

$t_kt_{k+2}+t_{k-1}t_{k+2}-t_{k+1}^2-t_kt_{k+1}$) (3.17)

v_{31}= s_{31} $(t_{k-1}^2-t_{k-2}t_k)$+ s_{32} $(t_k^2-t_{k-1}t_{k+1})$+ s_{33}(

$t_{k-1}t_{k+1}+t_{k-2}t_{k+1}-t_k^2-t_{k-1}t_k$) (3.18)

v_{32} = s_{31}($t_{k-2}t_{k+1}-t_{k-1}t_k$) + s_{32}($t_{k-1}t_{k+2}-t_kt_{k+1}$

)+ s_{33}($t_k^2+t_kt_{k+1}-t_{k-1}t_{k+2}-t_{k-21}t_{k+2}$) (3.19)

v_{33}= s_{31}($t_k^2-t_{k-1}t_{k+1}$) + s_{32}($t_{k+1}^2-t_kt_{k+2}$)+ s_{33}(

$t_kt_{k+2}+t_{k-1}t_{k+2}-t_{k+1}^2-t_kt_{k+1}$) (3.20)

Now calculating v_{11}

we have

v_{11} = ($c_1t_{k+2}+c_2t_{k+1}+c_3t_k$)($t_{k-1}^2-t_{k-2}t_k$) +

$(c_1(t_{k+1}+t_k)+c_2(t_k+t_{k-1})+c_3(t_{k-1}+t_{k-2}))$

($t_k^2-t_{k-1}t_{k+1}$) + ($c_1t_{k+1}+c_2t_k+c_3t_{k-1}$)

($t_{k-1}t_{k+1}+t_{k-2}t_{k+1}-t_k^2-t_{k-1}t_k$)

= $c_1.1 + c_2.0+c_3.0 = c_1$

using the fact that det T^{-k} = 1

Similarly, we get

$v_{12} = c_2$, $v_{13} = c_3$, $v_{21}= c_4$, $v_{22} = c_5$, $v_{23} = c_6$,

$v_{31} = c_7$, $v_{32} = c_8$ and $v_{33} = c_9$.

Now,

$$= \begin{bmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{bmatrix}^{e}$$

$$= \begin{bmatrix} c_1 & c_2 & c_3 \\ c_4 & c_5 & c_6 \\ c_7 & c_8 & c_9 \end{bmatrix}^{e}$$

$$= \left(\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix}^{d} \right)^{e}$$

$=(M^d)^e \ = M \bmod n.$

IV. SIMPLE EXAMPLE

Let us take a simple example to illustrate the proposed digital signature scheme. Suppose the message “DIGITAL SIGNATURES” is to be digitally signed. Assigning each letter with its position in the English alphabets as A =1, B =2 and so on, we get M= 4979201121997141202118519. Representing the message in the form of a square matrix M of order 3 X 3, we get

$$M = \begin{bmatrix} 49 & 79 & 201 \\ 121 & 997 & 141 \\ 202 & 118 & 519 \end{bmatrix}$$

We select prime’s p and q such that the determinant of M is relatively prime to n. Then, we perform the following steps.

Key generation

Let us take p = 31, q = 37 so that

n = p.q = 1147

$N = (p^3\text{-}1)\ (q^3\text{-}1) = \{(31)^3 \text{-}1)\ (37)^3 \text{-}1\}$

= 1508923080.

We select public key, e = 3127 such that

1 < 3127 < 1508923080 and

gcd (3127, 1508923080) = 1.

Then, private key is computed as

$d = (3127)^{-1} \bmod 1508923080 = 129274223.$

Signature generation

First, we check that determinant of message M is relatively prime to n.

$$\text{Here, } |M| = \begin{vmatrix} 49 & 79 & 201 \\ 121 & 997 & 141 \\ 202 & 118 & 519 \end{vmatrix} = -15781914$$

and gcd (15781914, 1147) =1

Let k = 4 be secret key,

$$\text{Computing } \alpha = T^4 = \begin{bmatrix} 7 & 6 & 4 \\ 4 & 3 & 2 \\ 2 & 2 & 1 \end{bmatrix} \text{ and}$$

$$\alpha^{-1} = T^{-4} = \begin{bmatrix} -1 & 2 & 0 \\ 0 & -1 & 2 \\ 2 & -2 & -3 \end{bmatrix}$$

The values of T^4 and T^{-4} are computed by using the relations (2.8) and (2.9)

Signature $S = M^d \bmod n.\ \alpha$

$$= \begin{bmatrix} 49 & 79 & 201 \\ 121 & 997 & 141 \\ 202 & 118 & 519 \end{bmatrix}^{1292742223} \bmod 1147 \ \text{x} \ \begin{bmatrix} 7 & 6 & 4 \\ 4 & 3 & 2 \\ 2 & 2 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 4767 & 4189 & 2617 \\ 4226 & 3445 & 2233 \\ 9381 & 8018 & 5244 \end{bmatrix}$$

Signature is now (S, α)

Signature Verification

$V = [S.\ \alpha^{-1}]^e \bmod n \ =$

$$\left(\begin{bmatrix} 47467 & 4189 & 2617 \\ 4226 & 3445 & 2233 \\ 9381 & 8018 & 5244 \end{bmatrix}\begin{bmatrix} -1 & 2 & 0 \\ 0 & -1 & 2 \\ 2 & -2 & -3 \end{bmatrix}\right)^{3127} \bmod 1147$$

$$= \begin{bmatrix} 467 & 111 & 527 \\ 240 & 541 & 191 \\ 1107 & 256 & 304 \end{bmatrix}^{17} \bmod 1147$$

$$= \begin{bmatrix} 49 & 79 & 201 \\ 121 & 997 & 141 \\ 202 & 118 & 519 \end{bmatrix} = \mathrm{M}$$

V. PERFORMANCE EVALUATION

The following notation is used to analyse the performance of the proposed scheme

T_{add} time for modular addition

T_{mul} time for modular multiplication

T_{exp} time for modular exponentiation

T_{sig} time for signature

T_{ver} time for verification

Computation of each signature and verification consists in calculation of 9 elements s_{11}, s_{12}, s_{13}, s_{21}, s_{22}, s_{23}, s_{31}, s_{32}, s_{33} and v_{11}, v_{12}, v_{13}, v_{21}, v_{22}, v_{23}, v_{31}, v_{32} and v_{33} respectively of the matrix which requires simple modular additions, exponentiations and matrix multiplications. The Signer needs 27 modular multiplications and 18 modular additions along with modular exponentiation time complexity to create a signature on any message M. The Signature validation verifier also needs the same computations for verifying the signature. Hence, we have

From equations 3.2 to 3.10 and 3.12 to 2.20

$$T_{sig} = 27T_{mul} + 18T_{add} + T_{exp} \qquad (4.1)$$
$$T_{ver} = 27T_{mul} + 18T_{add} + T_{exp} \qquad (4.2)$$

VI. CONCLUSION

In this paper, we presented a new Signature scheme based on factoring and Tribonacci matrices. Use of Tribonacci matrices increases the security of the scheme. For this, the message is also represented in the form of a square matrix of order 3. Computation using matrices reduces the key sizes and storage space without compromising the security. Also, the performance evaluation shows that the algorithm requires only simple modular additions and multiplications without any complex operations. Hence, the proposed scheme is more efficient than the existing schemes.

ACKNOWLEDGMENT

We thank the reviewers for their valuable comments for improvement of this paper.

REFERENCES

[1] W.-H. He, Digital signature scheme based on factoring and discrete logarithms, electronics *Letters*, 37 (2001) (4) pp. 220 – 222.

[2] Z. Shao, Signature schemes based on factoring and discrete logarithms, *IEE Proceedings-computers and Digital Techniques*, 145(1) (1998) 33–36,

[3] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* 21(2) (1978) pp. 120–126.

[4] Zekeriya Y. Karatas, Erkam Luy, Bilal Gonen, A Public Key Cryptosystem based on Matrices, International Journal of Computer Applications 182 (42) (2019).

[5] Indivar Gupta, Atul Pandey and Manish Kant Dubey, A key exchange protocol using matrices over group ring, Asian-European Journal of Mathematics 12(1) (2019).

[6] Mahalanobis A (2013) Are matrices useful in public-key cryptography. Int Math Forum 8:1939–1953 11.

[7] Mahalanobis A (2010). The discrete logarithm problem in the group of non-singular circulant matrices. Groups Complex Cryptol 2:83–39

[8] Saba Inam, Rashid Ali, A new ElGamal-like cryptosystem based on matrices over group ring, Neural Comput & Applic DOI 10.1007/s00521-016-2745-2

[9] A.P. Stakhov, The golden matrices and a new kind of cryptography, *Chaos, Solitons and Fractals*, 32 (2007) 1138-1146.

[10] Rakesh Nayak, Jayaram Pradhan, NTRU Digital signature scheme-A matrix approach, *International journal of Advanced Research in Computer science* 2(1) (2011).

[11] S.K. Rososhek, Fast and secure modular matrix based digital signature, British *journal of mathematics & computer science* 13(1) (2016) 1-20.

[12] Feras Bani-Ahmad, Mohd Taib Shatnawi, Nedal Tahat and Safaa Shatnawi, A new kind of digital signature scheme using Golden matrices based on factoring problem, International Journal of Pure and Applied Mathematics , 107(1) (2016) 49-57.

[13] M. Basu and M. Das, Tribonacci matrices and a new coding theory, *Discrete mathematics, Algorithms and Applications* 6(1) (2014).

[14] A. P. Stakhov, V. Massingue and A. Sluchenkova, *Introduction into Fibonacci coding and cryptography*, Kharkov, Osnova (1999).

[15] A.P. Stakhov, Fibonacci matrices, a generalization of the Cassini formula and a new coding theory, *Chaos, Solitons and Fractals* 30 (1) (2006) 56-66.

[16] A.P. Stakhov, A generalization of the Fibonacci Q-matrix Rep. *Nat. Acad. Sci.,Ukraine* (9) (2006) 46-9.